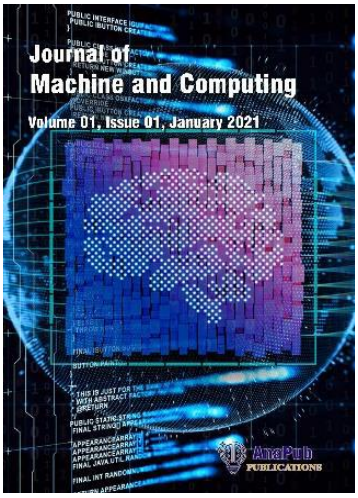
Journal Pre-proof



Data Protection and Security Management in the 6G Era: Addressing High-Density Cloud Computing Challenges

Xma R Pote, Hemavathi R, Anil Kumar N, Sheeba Santhosh, Krishnan T and Vidhya Prakash Rajendran

DOI: 10.53759/7669/jmc202505113

Reference: JMC202505113

Journal: Journal of Machine and Computing.

Received 10 July 2024

Revised form 02 February 2025

Accepted 05 May 2025

Please cite this article as: Xma R Pote, Hemavathi R, Anil Kumar N, Sheeba Santhosh, Krishnan T and Vidhya Prakash Rajendran, "Data Protection and Security Management in the 6G Era: Addressing High-Density Cloud Computing Challenges", Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505113.

This PDF file contains an article that has undergone certain improvements after acceptance. These enhancements include the addition of a cover page, metadata, and formatting changes aimed at enhancing readability. However, it is important to note that this version is not considered the final authoritative version of the article.

Prior to its official publication, this version will undergo further stages of refinement, such as copyediting, typesetting, and comprehensive review. These processes are implemented to ensure the article's final form is of the highest quality. The purpose of sharing this version is to offer early visibility of the article's content to readers.

Please be aware that throughout the production process, it is possible that errors or discrepancies may be identified, which could impact the content. Additionally, all legal disclaimers applicable to the journal remain in effect.

© 2025 Published by AnaPub Publications.

AnaPub
PUBLICATIONS

Data Protection and Security Management in the 6G Era: Addressing High-Density Cloud Computing Challenges

Mrs Xma R Pote[1]
Assistant Professor
Dept of Electrical Engg
Yeshwantrao Chavan College of Engineering
Nagpur Maharashtra
potexma@gmail.com

Dr. Hemavathi R[2]
Assistant Professor (SG),
Department of Computer Science and Engineering,
Saveetha School of Engineering,
Saveetha Institute of Medical and Technical Sciences,
Saveetha University, Chennai, India.
saihema01@gmail.com

Anil Kumar N[3]
Assistant Professor
Department of Electronics and Communication Engineering,
School of Engineering,
Mohan Babu University,
Tirupati, Andhra Pradesh, India
anil.kumar@mbu.asia

Sheeba Santhosh [4]
Assistant Professor Grade 1
Department of ECE
Panimalar Engineering College
drsheebas@panimalar.ac.in

T. Krishnan [5]
Assistant Professor
Koneru Lakshmaiah Education Foundation
tkrishnan.mtech@gmail.com

Mrs Vidhya Prakash Rajendran [6]
Lecturer
College of Engineering and Technology,
UTAS , NIZWA
vidhya.rajendran@utas.edu.om

Abstract

In the era of 6G, data safety and confidentiality are gravely threatened by the rise of dense cloud computing. The rise of high-density cloud computing has put previously unimaginable data processing, storage, as well as analytics capabilities within arms' reach. To make the most of data collected by sensors in different places, new 6G intelligence apps' training processes are in sync with federated learning paradigm. Because of high density cloud computing, distributed systems with hundreds or thousands of nodes can be deployed. This has potential to significantly impact data safeguarding and safety policy since it increases likelihood of harm to system from malicious actors. Encryption, access control, and defense layers are more advanced security techniques that are needed to keep confidential data safe in this environment. Encryption adds on another level of security by making it more difficult for those without permission to view information. Utilizing Secretary Bird optimization approach, optimal encryption key is selected. While access control prevents unauthorized users from reaching specific regions of system, defensive layers identify and thwart malicious attempts. This study suggests that 6G networks' data protection and security management could be improved with high density cloud computing. In order to address security concerns raised by encrypted data's lack of transparency, this paper proposes a mechanism for identifying data attacks on 6G intelligence apps that employ secure aggregation methods based on encryption. Our suite of encrypted data auditing solutions can protect you from data poisoning, incorrect data aggregation, and illegal data sources. On top of that, after evaluating a plethora of intriguing technologies, to have assessed each one and recommended optimal security practices for specific 6G scenarios.

Keywords: Data Storage; Security; Malicious Performers; Encryption; Data Protection; Cloud computing; Secretary bird optimization procedure.

Authors Pre-Proof

Introduction

Recklessly ignoring the increasing influence of the cloud on 6G broadband data security management and protection is not a viable option [1]. This innovation opened up numerous new possibilities for companies to operate their operations in the cloud, besides it has substantially improved data management and security [2]. The upcoming arrival of 6G networking in particular will meaningfully affect data protection and security management [3]. The arrival of cloud computing has greatly enhanced the security of data protection and the management of 6G network security. Because, data is now more reliable and accessible than ever before, and it's also more easier for individuals to use [4]. This skill has helped businesses reducing infrastructure expenses and improving cost efficiency. Cloud computing lets businesses to regulate which sections of their network have access to which data while yet taking advantage of economies of scale [5-6]. One advantage of cloud computing is the increased control it gives users over data sharing and storage. This is because cloud computing is more scalable and data saved in the cloud can be encrypted. Rapid advancement of networked technology, we are currently experiencing a digital shift. More and more high-density applications are using cloud computing, which has accelerated this trend [8].

Business-centric: This is because cloud computing does come with several advantages such as scalability, cost-effectiveness, and improved organizational agility. However, some businesses are concerned about security and anonymity of their data, which is a concern [9-10]. With proliferation of 6G networking and migration of data and apps to cloud, organizations are realizing need to update their data protection and security management solutions [11]. When it comes to data protection and security management, cloud computing offers numerous advantages, one of which is ability to store data safely in multiple layers of redundancy and protection [12]. In addition, cloud services can automatically offer data encryption and decryption. This encryption goes beyond what is currently available to protect sensitive information from eavesdropping [13–14]. While there are many benefits to cloud computing, increasing use of high-density cloud computing is creating new challenges for privacy and data security protocols [15]. Since more data is housed in fewer virtualized settings, attacks on data stored in these environments become more likely with high-density applications.

For 6G intelligence applications that rely on cryptography for secure aggregation, to present a data attack detection framework [16–17] to further tighten security. Encrypted data auditing techniques are a part of this framework that helps keep data safe from data poisoning, unauthorized sources, and errors in data aggregation. Furthermore, to assess and contrast numerous cutting-edge security techniques, shedding light on best ways to protect 6G networks from new cyber dangers. Optimising data protection, privacy preservation, and intrusion detection in the 6G future is the comprehensive goal of this article, which delves into the interplay between high-density cloud computing, federated learning, and data security. To show how these approaches can make next-gen wireless networks more efficient, reliable, and secure through thorough study. The article's main points are as follows:

Authors Pre-Proof

- Supernew phase of 6G. The first modern level of 6G shows the impact of the integration of ± of on 6G networks, allowing powerful encryption protocols here to improve encryption› security. Homomorphic encryption — a cloud-computing-based technology — can provide an end-to-end data security in the 6G networks.
- The Cloud: importance to security rules for 6G networks adaptive; The more common cloud computing → most importantly, adaptive security rules for 6G networks; Cloud;→ most importantly, adaptive security rules for 6G networks → cloud computing v v The significance of adaptive security rules for 6G networks will grow as cloud computing becomes more commonplace. Policies must not only safeguard data but also adapt to new situations and threats.
- Candidate 6G uses cloud systems which play a pivotal role in augmenting identity and access management. By implementing these identity management and access rules, you can provide additional layers of protection for sensitive data against unwanted access.
- Cloud computing increases accountability by providing fine-grained auditability, a necessary condition for maximum secure 6G networks. To monitor for deviations or any unauthorized access, cloud security systems log every action taken by every user, which can provide insight into insider threats or malicious employees

2. Related works

In his exploration of the synergy between FL and 6G networks, Chintha [18] highlights how this new paradigm can support distributed edge-device-based training of models with high levels of accuracy, making way for privacy-preserving AI. Communication overhead, data heterogeneity, and security risks are some of the issues discussed, along with possible solutions, for deploying FL within the 6G framework. By increasing security and decreasing the likelihood of data breaches, FL's incorporation into 6G networks has the potential to radically alter applications that deal with privacy concerns. Offering insights into the benefits, limitations, and future trajectory of privacy-preserving AI in next generation networks, this paper presents a complete overview of federated learning's role in 6G.

When it comes to public safety operations, Suomalainen et al. [19] has examined cybersecurity in intelligent tactical bubbles, which are autonomous, quickly deployable mobile networks. In addition to expanding the danger landscape, machine learning is crucial in quickly orchestrating these networks for various tasks and protecting them from new threats. Various threat and risk analysis approaches being investigated for their potential use in mission-critical networked systems. To provide the findings of a collaborative risk prioritisation analysis. Using the existing standardisation efforts for both terrestrial and non-terrestrial 6G as a foundation, to offer a security structure that employs the machine learning-based security fundamentals in top of protecting mission-critical assets on the network's edge.

In order to process, store, trace, and analyse data in a way that can aid in cost reduction, improved security, and consumer transparency, Osama et al., [20] has presented the usage of blockchain technology with many literature evaluations. Integrating blockchain's advantages with other breakthroughs can boost privacy, trust, and security. Additionally, to have examined the current state of data security in the cyber world and how blockchain technology might

Authors Pre-Proof

contribute to this advancement through its many useful characteristics. Lastly to discover future of blockchain technology in data in respect of velocity, efficacy, financial processes and designing smart contracts for companies. In addition, to unveiled the blockDADS framework, an all-encompassing paradigm for multi-layer integration of blockchain technology with data analytics and security.

Zhang et al. [21] have suggested new security measures to safeguard UxV networks and sensitive data. Combining UxVs with ML-based intrusion detection systems is one possible approach. The conventional approach can't handle the increased flexibility and possible decentralization of a 6G-based UxV network's security and privacy requirements. Furthermore, UxV clients can exhibit a high degree of variability when presented with training samples that are substantially uneven. Within a security-critical UxV environment, federated learning (FL) enables UxVs to collaborate on ML model training and updates while safeguarding user data. Cloud servers that help with intrusion detection and service delivery have been the focus of most of the decentralised approach research. This study introduces a decentralised FL framework with an emphasis on training machine learning models on UxVs for intrusion detection. This method may be more flexible than others because UxV clients can train and synchronize models without relying on a central server. The efficacy of the proposed approach was evaluated through the use of simulation experiments. The proposed method outperforms baseline models trained locally by clients and those utilizing FedAvg, according to both theoretical and experimental studies.

Xu et al. Regarding blockchain system's potential to secure data [22] This paper reviews the possible integration of machine learning (ML) methods to face the increasing complexity of handlings large amounts of data within a potential 6G framework. The hope is that this work will shed light on the latest techniques for securing data in vehicular communication systems. Read more in-depth on the results of a leading-edge infrastructure for confidentiality assessment of 6G network elements. This research study looks at the IoE and their noticeable implications with respect to internet security. It analyzes contemporary research issues regarding data privacy in the context of inter vehicle communication (IVC) in 6G. In order to address the data processing challenges of 6G wireless networks, our inquiry will include a look into ML approaches. According to the planned research, 6G wireless network conditions are getting more complex and changeable, which might make it tougher to communicate securely critical information. As it pertains to 6G networks, it shows how blockchain technology could be used to fix data security problems. Using ML technologies to manage the large data volumes of the 6G ecosystem is also highlighted in the paper as a potentially revolutionary possibility. The results show that these technologies are vital for reducing risks to data security in the 6G communication framework and guaranteeing confidentiality..

3. Threat Model

The implementation of 6G's built-in security measures guarantees that user data remains private. The invisible data made possible by data confidentiality protections is both a blessing and a curse, since it opens the door to new security dangers when different parties

Authors Pre-Proof

work together on analyses. 6G networks are a new kind of open-application networks that coexist with trustworthy, semi-trustworthy, and malevolent users. The latter group may try to harm the former by using the anonymity of encrypted data to their advantage during collaborative analysis.

3.1. Tampering attacks on the sealed/encrypted data

By feeding the central server changed ciphertexts on model parameters, malicious participants can manipulate the ciphertext aggregation process of the central server. It is possible for the central server to alter the model's aggregation results by changing the ciphertexts or aggregation weights while the model is being aggregated [23]. The central server might not get accurate aggregation results if data transfer or encryption/decryption operations are flawed.

3.2. Unencrypted Matters: Resale Attacks on Encrypted Data

Another major category of risks includes the vitiation of the blinded feature space (i.e., the encrypted representations of each data holder) and the information used to verify the shared data by malicious actors. By purposely using the homomorphic properties of existing models, malicious actors may create encrypted models that are suitable for federated learning. Since the parameters of the model are encrypted, the central server cannot determine whether a data holder participated in model resale or not. Federated learning is exposed to the involvement of malicious data holders that compromise the system even without training on computational resources [6].

3.3. Attacks by Poisoning on Encrypted Data

Anomalies in the global model could be caused by malicious data that rogue actors send to the central server. The central server cannot determine the exact roles played by each parameter in the aggregated model's performance or detect cases of data poisoning since model parameters are encrypted before aggregation.

3.4. Knock-Knock Attack on the Encrypted Data

Some dishonest users may try to steal the best aggregated model by sending in untrained models to the main server. The influence of each parameter on the aggregated model's performance and any freeloading or malicious actions inside the data cannot be determined by the central server since model parameters are encrypted before aggregation.

4. Proposed model

In this work, the brief explanation of proposed model on attack detection with privacy is mentioned in Figure 1.

Authors Pre-Proof

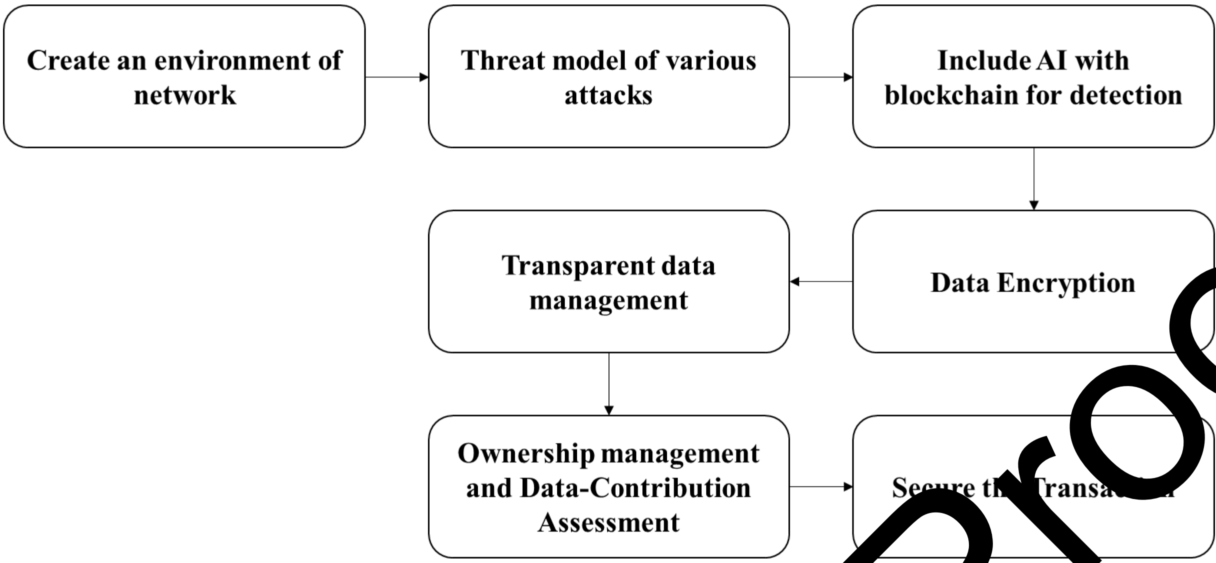


Figure 1: Workflow of the proposed perfect [illegible]

4.1. Blockchain and AI for Privacy and Data Protection

When combining blockchain with AI, data privacy and security should be the foremost concerns. A few key considerations are:

- Encrypt Sensitive Data: For any sensitive data being stored on a blockchain or having AI processes applied to it, ensure it is encrypted. Another dimension of security is data encryption, which protects the data itself from being accessed or read by someone who is not authorized to do so and does not possess the proper keys to decrypt the data.
- Pseudonymization: Pseudonymization techniques involve replacing real names, addresses, and other identifiers with fake ones so that the data can be processed and analyzed without risking the person's right to confidentiality.
- Access Control: Implement robust access control measures to ensure that data can only be accessed by authorized individuals or AI algorithms. Data read or write access is governed and the authentication takes place to make sure that no one besides the owner is able to access has access to the data.
- Adopt Privacy by Design: Follow a Privacy by Design methodology when developing blockchain and AI systems. In so doing, organisations can ensure that privacy comes upfront in a technology rollout by embedding elements and ideas of privacy as part of a design process.
- Data Minimisation: Only keep essential data needed to do your job If you value your privacy, and do not want your data to leak, then do not collect a data which is not necessary to do your job
- Manage Data Transparently: Blockchain is immutable and transparent, so data can be stored with track and control. You're putting the reins in the hands of people to use a blockchain technology, so they own their data — they have the power to know who's accessing it, when and how to delete it.
- Documentation & privacy policy: Keep users, stakeholders and staff informed about privacy regulations and policies. Demonstrate how they control individual data, how it

Authors Pre-Proof

can at first be both gathered and continuously transformed by the data that is securely stored by the Blockchain and AI frameworks.

- Regular Audits and Inspections – Do frequent clean audits and inspections at privacy and data protection level. And this process goes from the data management processes, through AI algorithms to blockchain infrastructure security

Thus, by incorporating data protection and privacy measures during the design and implementation phase of blockchain and AI systems, organisations can achieve a good degree of privacy while achieving certain benefits from either or both systems. Adopting a privacy-conscious data strategy, undergoing regular reviews for compliance with the then-current rules and best practices, and making sure your organization is compliant.

4.2. Authentication against Ciphertext Resale Attacks of User Data Ownership

However, since all models are encrypted before the aggregation of model parameters in a 6G environment, the central server in federated learning is unable to immediately verify the identity of the sender of model parameters [236]. Malicious players in such settings can obtain the learning for free by stealing and selling the encrypted models of other participants, thus, contributing to the learning without paying for the computational resources. This demotivates training. In an effort to mitigate this challenge, this work proposes a Pedersen commitment-based user data-ownership authentication mechanism. In this way, the service provider initiates a challenge that can only be answered correctly by the legitimate data owners, which they can do by demonstrating they possess the plaintext data that corresponds to the ciphertext.

Additionally, it is possible to determine whether some data has been illegally resold or modified without decrypting specific model limits by combining the aggregative commitment verification procedure which is based on Σ-protocol. As opposed to its previous technologies, this technology utilizes 6G's reduced latency and greater dependability to optimize the process of data interchange in a secure manner. It guarantees the integrity of both data and participants themselves during the federated-learning phase. With such a large capacity and high bandwidth, dynamic trust evaluations work wonderfully. Here are some of the key ideas we have for this sophisticated network setting about data ownership authentication:

Every piece of data should be encrypted and a promise should be made to prove who owns it and where it came from, according to the encryption and principle. By doing so, data owners can verify the data's authenticity and integrity while also protecting the original information. 6G's extreme low latency and plentiful applications with high bandwidth capability allow us to speed up the verification of encrypted data and commitments now. Data owners can demonstrate control and ownership of the data without revealing it to anyone by committing C to a central server, using the formula C=g^r h^m in the data-ownership authentication scheme. Along with commitment knowledges, encryption is a powerful tool for confirming data ownership and protecting data privacy.

To put it short, as governed by the audit mistake detection and audit traceability principle of data-ownership audit, if the first verification fails, the audit can be reconfigured

Authors Pre-Proof

for finer things, for specific data owners. Audit data can be collected and processed quickly, and errors can be identified and tracked in real-time, all thanks to lightning-fast data transfer 6G will provide. In the data-ownership authentication system, the central server checks the validity of each data owner promise with the formula If errors or mismatches are found at this stage, the central server can choose which data owners to re-audit and do a more detailed grouped aggregate audit to find the source of the problem. This achieves efficient error detection and traceability by detecting specific faults and tracing them back to individual data owners.

4.3. Ciphertext Data-Contribution Assessment for Poisoning and Free-Riding Attacks

The characteristics mentioned above, together with the encrypted model parameters in ciphertext before aggregation, make it difficult for us to directly assess data quality or accurately locate harmful data in federated learning. Our method uses a ciphertext data-contribution evaluation strategy for protecting aggregated data based on dual-trapdoor encryption and is able to employ the potentials of 6G communication technology to protect against passive attacks from data holders. This approach adds noise to model parameters taking advantage of well-encrypted user data for much better performance. Specifically, due to the dual-trapdoor homomorphic features, the noises can maintain cancelling each other during the aggregation process, thus the real value of the datum does not change with the addition of the injected noise. Also, the article applies a group aggregation-based approach for locating fraudulent users. Final calculations of the results, gathered and decrypted data over multiple groups using the lightning fast processing capability of 6G. We can mark a participant that always does poorly in every group relative to model accuracy as potentially low-contributing. This method can identify malicious attackers by enhancing data security and model quality during federated learning.

Every evaluation of data contribution has to be verifiable, according to the verifiability principle. It is important that all evaluation outcomes may be independently checked for correctness and fairness. To can verify data-contribution assessments in real-time with 6G's ultra-low latency capabilities. Broader data synchronisation and sharing is possible with 6G networks' extended connectivity and higher bandwidth, which enhances system transparency.

Encrypted gradient data is utilised in through the joint audit method. C_{ij} from each data owner decrypted, obtaining the actual gradient contributions m_i^r and m_j^c, where the procedures can be independently checked, and the evaluation findings may be seen by anybody in the public eye and checked by any auditor or third party, in accordance with the principle of verifiability. According to the fairness principle, it doesn't matter how big or bad a participant's data set is; what matters is that their encrypted data contribution evaluation accurately reflects their real contributions. To guarantee equitable distribution of resources and incentive mechanisms, the evaluation algorithm has to correctly differentiate and measure the worth of various contributions. By quickly adjusting assessment algorithms and criteria, 6G ensures that assessments are fair and up-to-date with participant contributions and the most recent data. This, in turn, optimises resource allocation and ensures that everyone benefits equally. Following the format utilised in the data-contribution evaluation system,a if $L_i^r - L_{ij} > \epsilon_3$ and

Authors Pre-Proof

$L_j^c - L_{ij} > \epsilon_3$, Devices are deemed free riders if their actual data contribution is shown to be greater than their stated contribution, which is determined by comparing the two.

To keep things fair, this stage makes sure that everyone gets rewards and resources based on what they actually contribute in terms of data.

4.4. Finding The Optimal Key using Secretary Bird Optimization Algorithm (SBOA)

This study introduces SBOA, a tool for finding the optimal key of the encryption model. What follows is a proposal to offer SBOA with a mathematical model of the secretary birds' natural behaviour as it pertains to natural enemies [24].

4.4.1 INITIAL PREPARATION PHASE

One example of a population-based metaheuristic technique is the Secretary Bird Optimisation Procedure (SBOA), in which every Secretary Bird is essentially a member of the algorithm's populace. The values of the decision variables are determined by the positions of each space. Therefore, under the SBOA technique, the Secretary Birds' positions stand for potential answers to the problem. To randomly initialise the placements of the Secretary Birds space, the first SBOA implementation uses Eq. (1).

$$X_{i,j} = lb_j + r \times (ub_j - lb_j), i = 1,2, \ldots Dim \quad (1)$$

where X_i signifies the position of bird i, lb_j and ub_j are the bounds, correspondingly, besides r represents a random sum among 0 besides 1.

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & x_{1,j} & \cdots & x_{1,Dim} \\ x_{2,1} & x_{2,2} & x_{2,j} & \cdots & x_{2,Dim} \\ x_{3,1} & x_{3,2} & x_{3,j} & \cdots & x_{3,Dim} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{N,1} & x_{N,2} & x_{N,j} & \cdots & x_{N,Dim} \end{bmatrix}_{N \times Dim} \quad (2)$$

X said secretary bird group, X_i bird, $X_{i,j}$ The ith secretary asked the jth inquiry about the variable's rate in Nth member of the group (the secretary) brought up the issue of the variable's dimension, and Dim brought it up as well.

A potential optimisation solution is represented by each bird. As a result, to may test the objective function using the values that each secretary bird has suggested for the problem variables. Equation (3) is then used to compile the resultant values of the goal function into a vector.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N \times 1} = \begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N \times 1} \quad (3)$$

Authors Pre-Proof

In this case, F is that the ith secretary bird got. One way to find best possible solution to a problem is to compare the functions that were calculated. This allows one to evaluate the quality of each prospective solution. The solution for a minimization problem is the secretary function value; for a maximisation problem, the best candidate solution is the greatest value. Each iteration updates the objective function values and the secretary birds' positions, therefore it's important to choose the best candidate solution every time.

In order to keep the SBOA members informed, to have used two separate secretary bird behaviours. The scope of these two categories of actions includes:

(a) The typist bird's hunting approach;
(b) The plan for the secretary bird to get away.

As a result, there are two steps to updating the secretary bird colony every time around.

4.4.2 Hunting Approach of Secretary Bird (Exploration Stage)

Secretary birds usually go through food: locating prey, eating prey, and then resting. Based on the biological facts of the stages and their durations, the secretary bird's hunting operation was divided into three equal segments. In particular, $t < \frac{1}{3}T, < \frac{1}{3}T < t < \frac{2}{3}T \; and \; < \frac{2}{3}T < t < T$ The secretary bird's hunting behaviour consists of three stages: seeking, eating, and attacking. So, here is how SBOA simulates each procedure:

Stage 1 (Searching for Prey): The secretary bird's hunting strategy begins with the discovery of prey, such as snakes. Because of their exceptional vision, secretary birds can spot snakes moving at the speed of light across the vast savannah. They use their long legs to swish the ground as they carefully look for signs of snakes. Because of their lengthy limbs, they are able to maintain a safe distance from serpents, protecting themselves from attacks. When investigating novel avenues becomes crucial during initial optimization cycles, this phenomenon occurs. That is why a differential evolution approach is used at this point. The goal of differential evolution is to enhance algorithm search skills by generating novel solutions based on individual differences. Differential mutation techniques are one method that diversity employs to evade local optima traps. Encouraging people to investigate different parts of the solution space increases the possibility of finding. So, we can mathematically depict the secretary bird's process of updating its site during the Searching for Prey phase using Eqs. (4) and (5)..

$$While \; t < \frac{1}{3}T, x_{i,j}^{newP1} = x_{i,j} + \left(x_{random\_1} - x_{random\_2}\right) \times R_1 \quad (4)$$

$$x_i = \begin{cases} X_i^{new,P1}, & if \; F_i^{new,P1} < F_i \\ X_i, & else \end{cases} \quad (5)$$

where, t characterises repetition quantity, T typifies extreme iteration sum, $X_i^{new,P1}$ embodies bird in the first phase, then x_{random_1} and x_{random_2} proposed answers during the arbitrarily produced array of dimensions 1 × Dim, where Dim is the space, and the intermission

Authors Pre-Proof

[0, 1] is used. $X_i^{new,P1}$ Signifies its charge of jth dimension, and $F_i^{new,P1}$ characterises its function.

Stage 2 (Consuming Prey): A secretary bird's hunting style takes a bizarre turn the moment it finds a snake. The secretary bird is able to out-smart the serpent because it uses its deft flight technique rather than charging headfirst into combat. From its perch above, the secretary bird maintains a careful watch on the serpent. It can hover, jump, and discreetly bother the serpent, draining its energy, all because it watches the snake's movements so well. This is where Brownian motion (RB) comes into play; it will allow us to simulate the secretary bird's erratic flight patterns. It is possible to model Brownian motion numerically using Eq. (6). The secretary bird achieves a significant physical advantage by utilizing this "peripheral combat" strategy. This bird's long legs make it difficult for snakes to entangle itself, and the thick keratin scales that cover its legs and talons provide protection from the fangs of deadly snakes. Now and then, the secretary bird will pause what it's doing and fix its intense gaze on the serpent. In order to use Brownian motion and the concept of "xbest" (the best possible location) in this particular setting. Users can zero in on the best position they've found so far in their local searches using "xbest," enabling them to explore the solution space even more. This approach not only helps people postpone convergence to local optima, but it also expedites the optimal solution space locations. Reason being, by combining global data with past best locations, individuals increase their chances of finding the global optimum. When dealing with complex problems, adding an element of uncertainty improves results because it provides people more opportunities to break out of their comfort zones and find better solutions. So, we can mathematically depict the secretary bird's procedure of altering its location in the Overwhelming Prey stage by applying Eqs. (7) and (8)..

$$RB = randn(1, Dim) \quad (6)$$

$$While\ \frac{1}{3}T < t < \frac{2}{3}T\ x_{i,j}^{newP1} = x_{best} + exp\left((t/T\wedge 4) \times (RB - 0.5) \times \left(x_{best} - x_{i,j}\right)\right) \quad (7)$$

$$X_i = \begin{cases} X_i^{new,P1}, & if\ F_i^{new,P1} < F_i \\ X_i, & else \end{cases} \quad (8)$$

The array with dimensions 1 × Dim and a standard deviation of 1 is represented by randn(1, Dim), while the current top value is denoted by xbest..

Stage 3 (Attacking Prey): As the snake nears its end, the secretary bird seizes the moment with its powerful leg muscles. The secretary bird will then swiftly raise its leg and aim its sharp talons at the snake, typically aiming for its head, before beginning to kick it. Quickly incapacitating it so you can avoid its bite is the objective of administering these kicks. The snake is immediately killed as the lethal sting of the talons lands squarely on its most vulnerable area. Occasionally, the secretary bird will let a snake go into the sky and then let it crash to the ground when it grows too large to be killed immediately. Adding the Levy flight strategy to search procedure will boost search capabilities, lower the possibility of SBOA solutions, and improve accuracy. The unpredictable gait pattern called Levy flying is

Authors Pre-Proof

characterized by short, steady steps punctuated by uncommon large jumps. By mimicking its flight qualities, it enhances the secretary bird's search powers. While small steps improve optimization accuracy, large steps allow the algorithm to more efficiently traverse the whole search space, bringing people closer to the optimal position. For SBOA to be more adaptable throughout optimization, it should incorporate a nonlinear perturbation component represented as. As a result, SBOA will be able to optimize method presentation, minimize early convergence, and achieve a better balance among exploitation. $\left(1-\frac{t}{T}\right)(2\times\frac{t}{T})$ Therefore, bird's site in Attacking established using Eqs. (9) and (10).

$$While\ t > \frac{2}{3}T, x_{i,j}^{new1} = x_{best} + \left(\left(1-\frac{t}{T}\right) \wedge \left(2\times\frac{t}{T}\right)\right) \times x_{i,j} \times RL \ (9)$$

$$X_i = \begin{cases} X_i^{new,P1}, if\ F_i^{newP1} < F_i \\ X_i, \quad\quad\quad else \end{cases} (10)$$

Using the flight, or RL for short, improves the algorithm's optimization accuracy..'

$$RL = 0.5 \times Levy(Dim)\ (11)$$

Here, Levy(Dim) is the notation for the Levy flight. It is calculated in this way::

$$Levy(D) = s \times \frac{u\times\sigma}{|v|^{\frac{1}{\eta}}}\ (12)$$

The memory bank is a set of normalized feature representations. Whereas ID uses instance labels to train a model, SD uses segment labels instead. When using M segments in SD,

$$\sigma = \left[\frac{\Gamma(1+\eta)\times sin\left(\frac{\pi\eta}{2}\right)}{\Gamma\left(\frac{1+\eta}{2}\right)\times\eta\times 2\left(\frac{\eta-1}{2}\right)}\right]^{\frac{1}{\eta}}\ (13)$$

Here, Γ indicates function besides η has a charge of 1.5.

4.4.3 Escape Policy of Secretary Bird (Exploitation Phase)

These are among the most dangerous animals that secretary birds must contend with. The birds are vulnerable to attacks and predation by these creatures. When secretary birds encounter these threats, they typically employ a range of avoidance strategies to protect food. These broadly classified into two categories. The first move is to run or take flight. Secretary birds are able to run at astonishing rates due to their exceptionally long legs. One reason they're dubbed "marching eagles" is that they may cover 20–30 kilometers on foot in a single day. In addition, secretary birds are excellent fliers, allowing them to swiftly take flight and seek refuge from danger. The second strategy is to blend in. In order to avoid danger, secretary birds can use structures or colors that fit in with their environment. Two events are considered equally likely to occur in the SBOA.:

i. C1: Camouflage by situation;

ii. C2: Fly or run away.

Authors Pre-Proof

When a secretary bird senses a predator is near, its first move is to seek cover. With no safe haven in the area, they will opt to escape away. Therefore, in order to supply a component, $\left(1-\frac{t}{T}\right)^2$ By adjusting for this variable, the process is able to strike a balance between exploring (seeking for new answers) and exploiting (making the most of current ones). Changing these variables at specific moments allows you to boost exploitation or raise the bar for exploration. The two evasion secretary birds may be described using Eq. (14), and this revised condition is expressed in Eq. (15).

$$X_{i,j}^{new,P2} = \begin{cases} C_1: x_{best} + (2 \times RB - 1) \times \left(1-\frac{t}{T}\right)^2 \times x_{i,j}, & if\ r\ and < r_i \\ C_2: x_{i,j} + R_2 \times \left(x_{random} - K \times x_{i,j}\right), & else \end{cases} \quad (14)$$

$$X_i = \begin{cases} X_{i,j}^{new,P2}, if\ F_i^{new,P2} < F_i \\ X_i, \quad else \end{cases} \quad (15)$$

In this case, r=0.5, R2 is the characteristic of the random standard distribution, x_random is the randomly generated solution for this iteration, and K are the integers 1 and 2, which can be found using Eq. (16).

$$K = round(1 + rand(1,1)) \quad (16)$$

Here, $rand(1,1)$ means haphazardly making a random (0,1).

4.4.4 Algorithm Complexity Analysis

Because various algorithms take different amounts of time to optimize similar issues, it is critical to evaluate an algorithm's computational difficulty before deciding how long it should run. In this paper, we use Big O notation to look at the time complexity of SBOA. If the population size of secretary birds is N, then the maximum number of iterations is T, and the dimensionality is Dim. The time complexity of randomly initializing the population is O(N), as stated by the laws of number O. The computing difficulty of updating the solution, which involves updating all feasible repair sites, is O(T × N) + O(T × N × Dim). From this, we can deduce that computational burden of the suggested SBOA is as $O(N \times (T \times Dim + 1))$.

5. Experiments Evaluation

5.1. Secure Aggregation Data Correctness Verification

Using the MNIST and Celeb A datasets, deep-learning models for picture recognition are trained in this part. Ten central processing unit (CPU) servers, each with sixteen cores, are used to mimic one central server and to train representations using the MNIST dataset. Data holders in batches undergo training on the Celeb A dataset model on a single GPU server equipped with eight 16 GB NVIDIA TESLA T4 GPUs. Data supported by the Charm-crypto (0.5.0) besides Numpy (1.18.5) libraries, while the PyTorch (1.6.0). Experimental time is measured in seconds.

There will be considerably more connected devices, faster communication speeds, and larger data volumes in the 6G environment than in the current state of the art. Due to the unique

Authors Pre-Proof

challenges posed by networks, methods for ensuring the accuracy of both efficient and secure. In Table 1 you can see a comparison of how well different encryption methods work.

Table 1. Evaluate different encryption algorithms' performance. "↢" means that the matching feature has been activated.

Method	Correctness	Privacy	Efficiency	Scalability
ZKP	√	√		
Paillier	√	√		
SMPC	√	√		√
MTH	√			√
ATH	√		√	√
Blockchain	√		√	

5.1. Analysis of proposed classical with existing procedures

Table 2 and Figure 2 presents the performance of the projected classical with existing techniques in accuracy, where processing time is mentioned in Table 3.

Table.2. Assessment of accuracy

No. of rounds	SMPC	ABE	IDS	TEE	Proposed
200	82.28	95.54	71.39	82.26	92.47
400	83.29	96.67	74.32	83.52	94.94
600	84.77	97.02	75.86	85.41	95.74
800	85.76	[illegible]	77.89	86.61	96.94
1000	86.88	99.74	78.79	87.16	97.58

Assessment of Accuracy compares the accuracy of different security models—SMPC, ABE, IDS, TEE, and the Proposed model—across varying numbers of rounds. The Proposed model consistently achieves high accuracy, starting at 92.47% for 200 rounds and reaching 97.58% at 1000 rounds, indicating its robustness and reliability. ABE outperforms all models, with accuracy reaching 99.74%, but likely at a higher computational cost. IDS maintains the lowest accuracy, suggesting its limitations in secure processing. TEE and SMPC offer moderate performance but are outclassed by the Proposed model. The Proposed model achieved good results and demonstrates the ability of our proposed model to achieve a trade-off between accuracy and computational cost.

Authors Pre-Proof

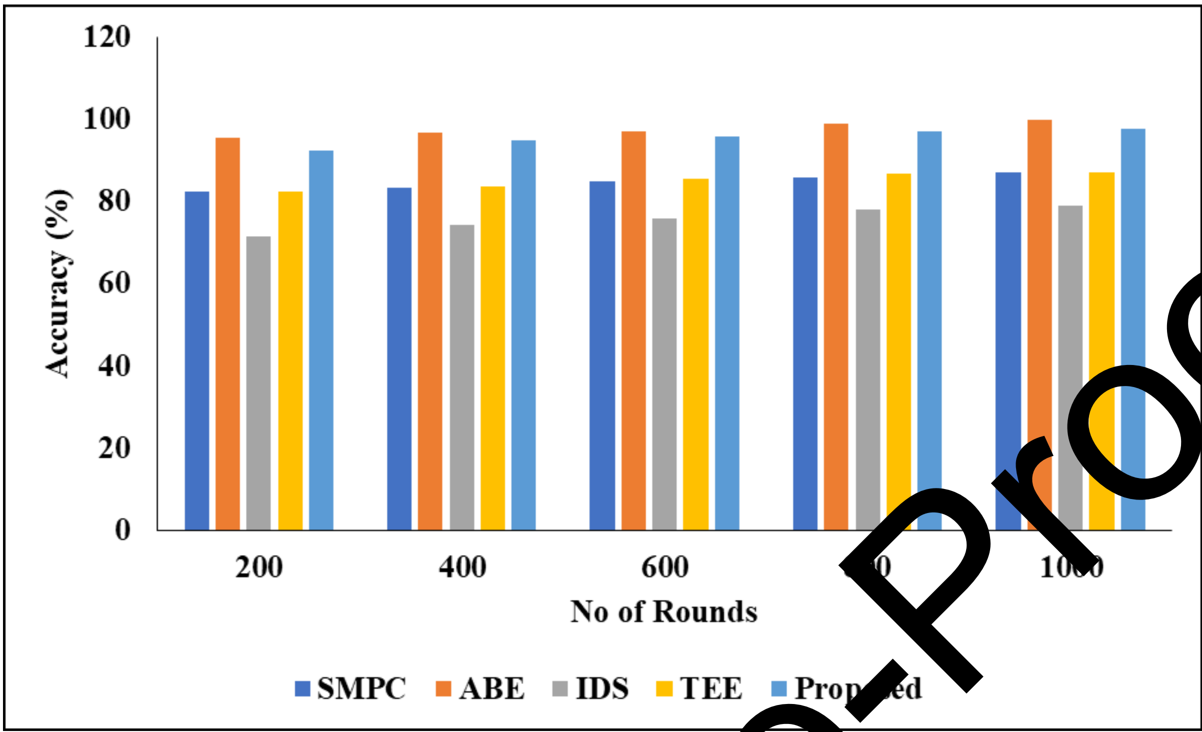


Figure 2: Study of proposed model with existing procedures

Table.3. Comparison of processing time

No. of rounds	SMPC	ABE	IDS	TEE	Proposed
200	84.28	93.54	73.39	80.26	90.47
400	85.29	94.67	76.32	81.52	92.94
600	86.77	95.02	77.86	83.41	93.74
800	87.76	[illegible]	79.89	84.61	94.94
1000	88.88	97.74	80.79	85.16	95.58

Comparison of Processing Time analyzes all the security models (SMPC, ABE, IDS, TEE, Proposed model) according to the rounds of processing, where the number increases. We can see that the Proposed model consistently outperforms SMPC, IDS, and TEE in terms of processing efficiency, although it is slightly inferior to ABE in absolute values. As the number of rounds grows, the processing time of the Proposed model increases from 90.47 at 200 rounds to 95.58 at 1000 rounds, demonstrating the scalability of the approach. The processing times for ABE seem to be the most varied and largest, while the processing times for IDS across all rounds are the smallest and most consistent, revealing that IDS is the lightest processing method that lacks robustness. The Proposed model exhibits such characteristics for its better efficiency-security trade-off, making it a perfect competitor for the implementations.

5.2. Period of Encryption and Decryption analysis

The planned model encryption and decryption time are compared with the existing techniques in Table 4 and 5.

Authors Pre-Proof

Table 4: Encryption time

Encrypted Message Length (bit)	30	50	100	200	300
BCP_MK_Dec	4.86	4.87	4.87	4.87	4.88
Paillier_Dec	2.79	2.92	3.4	4.12	4.88
Proposed	0.25	0.25	0.25	0.25	0.25

The Encryption Time Analysis I divide the encryption times of different encryption algorithms for procedures based on different length of message. Based on the results shown in Table 5, we can see that the Proposed model keeps an impressively large encryption time of 0.25 under all bit lengths, which performed highest when it is compared against Paillier_Dec and BCP_MK_Dec. In the case of Paillier_Dec, there is an upward trend in encryption time with the increase of message length (between 2.794 and 4.882), BCP_MK_Dec remains relatively stable (4.862, 4.868), while the Proposed model achieves great efficiency, making it an excellent choice for requests that need rapid encryption with lower computational overhead.

Table 5. Archive time input of encryption process.

Decrypted Message Length (bit)	30	50	100	200	300
BCP_MK_Dec	9.77	9.78	9.78	9.78	9.78
Paillier_Dec	7.34	7.34	7.34	7.34	7.34
Proposed	4.87	4.87	4.87	4.87	4.87

Decryption Period Consumption for Every Encryption Procedure illustrates a comparison of decryption time through different encryption techniques across different sequences of the message length. The Contrast model significantly outperforms other methods, as shown in Fig. 9. On the other hand, Paillier_Dec has a steady but comparatively high decryption time of 7.34 while BCP_MK_Dec is persistent and slowest with a constant 9.78. This proves that the proposed method is more efficient and computational expense reduced to be a better choice of scenarios that need rapid decrypting.

6. Conclusion

6G networks and computing have transformed data storage, processing, and security ordering. Although these advances allow for scalable and efficient distributed intelligence systems, they create major cybersecurity challenges to overcome. Data breach causes and unauthorized access, also adversarial attacks and so on will result in risks, accordingly the need to develop a strong encryption mechanism access control strategies and multi-layered

Authors Pre-Proof

defensive architecture. In this study, applications, By integrating encrypted-data auditing techniques, our framework effectively mitigates data- unauthorized data sources, thereby enhancing the security and reliability of 6G-based AI-driven applications. Furthermore, to analyzed and compared multiple security approaches, recommending optimal strategies for securing high-density cloud computing environments. Our findings demonstrate that implementing advanced encryption techniques, AI-driven intrusion detection systems, and federated learning paradigms can significantly improve data security in 6G networks. Moreover, the Secretary Bird Optimization Algorithm enhances cryptographic key selection, ensuring a higher level of data protection. These security measures contribute to resilient, privacy-preserving, and efficient 6G infrastructures, safeguarding against evolving cyber threats. Future integration of quantum cryptography and blockchain technology will enhance the security of 6G networks by ensuring ultra-secure communication and decentralized trust management in federated learning systems. Additionally, the development of AI-powered IDS and adaptive security frameworks that leverage deep learning for real-time anomaly detection will be critical in mitigating evolving cyber threats.

Reference

[1] Li, C. (2024). Privacy-Preserving of Digital 6G IoT Based Cyber Phycical System in Medical Big-Data Application Using Homomorphic Encryption. Wireless Personal Communications, 1-14.

[2] Mageshwari, M., & Naresh, R. (2024). Security Clouds to Improve Privacy and Conduct Continuous Audits in 6G Networked Environments Smart Cities. Wireless Personal Communications, 1-24.

[3] Dass, P., Ujjwal, S., Novotny, J., Zolotavkin, Y., Laaroussi, Z., & Köpsell, S. (2024, August). Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects. In Annual Privacy Forum (pp. 87-111). Cham: Springer Nature Switzerland.

[4] Rachakonda, L. P., Siddula, M., & Sathya, V. (2024). A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). High-Confidence Computing, 100220.

[5] Sun, Z., Liang, J., Yin, L., Xu, P., Li, C., Wan, J., & Wang, H. (2024). A Data Attack Detection Framework for Cryptography-Based Secure Aggregation Methods in 6G Intelligent Applications. Electronics, 13(11), 1999.

[6] Patil, S., Satya, A. D. V., Bajjuri, U. R., Damarapati, P. K., Manur, M., Thirumalraj, A., & Tambeti, R. (2024). Advancements in Deep Learning Techniques for Potato Leaf Disease Identification Using SAM-CNNet Classification. Ingénierie des Systèmes d'Information, 29(5).

[7] Yuvarani, R., & Mahaveerakannan, R. (2024, July). Payment Security Expert: Analyzing Smart Cards and Contactless Payments with Cryptographic Techniques. In 2024 2nd

Authors Pre-Proof

International Conference on Sustainable Computing and Smart Systems (ICSCSS) (pp. 511-516). IEEE.

[8] Laaroussi, Z., & Köpsell, S. (2024). Addressing Privacy Concerns in Joint Communication and Sensing for 6G Networks: Challenges and Prospects. In Privacy Technologies and Policy: 12th Annual Privacy Forum, APF 2024, Karlstad, Sweden, September 4–5, 2024, Proceedings (Vol. 14831, p. 87). Springer Nature.

[9] Parra-Ullauri, J. M., Zhang, X., Bravalheri, A., Moazzeni, S., Wu, Y., Nejabati, R., & Simeonidou, D. (2024). Federated Analytics for 6G Networks: Applications, Challenges, and Opportunities. IEEE Network.

[10] Gkonis, P. K., Nomikos, N., Trakadas, P., Sarakis, L., Xylouris, G., Masip-Bruin, X., & Martrat, J. (2024). Leveraging network data analytics function and machine learning for data collection, resource optimization, security and privacy in 6G networks. IEEE access, 12, 21320-21336.

[11] Rajalakshmi, B., Thirumalraj, A., Anandhi, R. J., & Khodadadi, N. (2024). Automated Spam Detection Using ECSA-Based Feature Selection with DGRN Classifier in Soft Computing Applications. In Soft Computing in Industry 5.0 for Sustainability (pp. 225-244). Cham: Springer Nature Switzerland.

[12] Sridharan, S., Deivasigamani, S., Rajesh, [illegible], & Surendran, R. (2024, July). Enhancing healthcare through AI deep learning: a human-centric IoT advisory system cloud. In 2024 2nd international conference on sustainable computing and smart systems (ICSCSS) (pp. 346-350). IEEE.

[13] Liu, H., Wang, Y., & Jia, F. (2024). Security and Privacy Protection of Internet of Things Devices in 6G Networks. International Journal of System Assurance Engineering and Management, 1-18.

[14] Fachrurrozi, N. [illegible], [illegible], K., & Anwar, K. (2024, November). Challenges on Security and Privacy in IMT-2030 (6G) Networks. In 2024 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT) (pp. 691-698). IEEE.

[15] Falola, P. B., Adeniyi, E. A., Awotunde, J. B., Jimoh, R. G., & Imoize, A. L. Security challenges and prospects of 6G network in cloud environments. Security and Privacy Schemes for Dense 6G Wireless Communication Networks, 471.

[16] Sivakumar, T. B., Hasan Hussain, S. H., & Balamanigandan, R. (2024). Internet of Things and Cloud Computing-based Disease Diagnosis using Optimized Improved Generative Adversarial Network in Smart Healthcare System. Network: Computation in Neural Systems, 1-24.

[17] Mallikarjunaradhya, V., Yennapusa, H., Palle, R. R., Suganyadevi, K., & Gupta, N. (2024, March). Impacts of high denisty Cloud Computing on Data Protection and Security management for 6G Networking. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 617-622). IEEE.

Authors Pre-Proof

[18] Chintha, V. R. Federated Learning for Privacy-Preserving AI in 6G Networks, Vol. 13, Issue: 01, January: 2025 (IJRMEET) ISSN (o): 2320-6586.

[19] Suomalainen, J., Ahmad, I., Shajan, A., & Savunen, T. (2025). Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence. Future Generation Computer Systems, 162, 107500.

[20] Osama, O. F., Bhusal, B., Kshetri, N., & Pokharel, B. P. (2025). blockDADS: Blockchain Technology for Data Analytics and Data Security–Applications and Solutions. In Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures (pp. 222-234). CRC Press.

[21] Zhang, J., Luo, C., Jiang, Y., & Min, G. (2025). Security in 6G-Based Autonomous Vehicular Networks: Detecting Network Anomalies With Decentralized Federated Learning. IEEE Vehicular Technology Magazine.

[22] Xu, T., Wang, N., Pang, Q., & Zhao, X. (2024). Security and privacy of 6G wireless communication using fog computing and multi-access edge computing. Scalable Computing: Practice and Experience, 25(2), 770-781.

[23] Gunapriya, B., Thirumalraj, A., Anusuya, V. S., Kavin, B. P., & Seng, G. H. (2024). A Smart Innovative Pre-Trained Model-Based QDM for Weed Detection in Soybean Fields. In Advanced Intelligence Systems and Innovation in Entrepreneurship (pp. 262-285). IGI Global.

[24] 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), 1-102.

Authors Pre-Proof