Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Tiger Hash Key (THK) Assisted Goat Optimisation Algorithm (GOA) for Intrusion Detection and Privacy Preserving of Electronic Health Records (EHR) in Distributed Cloud Data Environment

[1]A Sathya, Sri ,[2]V Jeevika Tharini, [*3]A Aruna, Sri Ramachandra ,[4]Anamika Raj, [5]N.Ambika devi

[1] Ramachandra Faculty of Engineering and Technology, Sri Ramachandra Institute of Higher Education and Research (DU), Chennai.

[2] Sri Ramachandra Faculty of Engineering and Technology, Sri Ramachandra Institute of Higher Education and Research (DU) , Chennai.

[*3] Faculty of Engineering and Technology, Sri Ramachandra Institute of Higher Education and Research (DU), Chennai. arunaarulmani@gmail.com (Corresponding Author)

[4] Department of Computer Science, Applied College Al Mahala, 61421, King Khalid University, Saudi Arabia.

[5] Department of Information Technology, Nadar Saraswathi College of Arts and Science, Theni.

Cite this paper as: A Sathya, Sri ,V Jeevika Tharini, A Aruna, Sri Ramachandra ,Anamika Raj, N.Ambika devi (2024). Tiger Hash Key (THK) Assisted Goat Optimisation Algorithm (GOA) for Intrusion Detection and Privacy Preserving of Electronic Health Records (EHR) in Distributed Cloud Data Environment. *Frontiers in Health Informatics, 13* (3), 950-963.

Abstract

The emergence of the cloud environment necessitates privacy preservation and trust assurance that paves the way to embark on new privacy-preserving techniques. Novel and efficient privacy preservation techniques give users confidence in evolving issues relevant to privacy and cyber-related risks. In this research work, trust mode, robustness evaluation for unique key, and Tiger Hash Key (THK) generation mechanism assisted Goat Optimisation Algorithm (GOA). The Cloud Service Provider (CSP) trust is determined by the trust model, which is an essential process in Cloud Computing (CC) and the selection of CSP for further storage as well as the process of Electronic Health Record (EHR) data. The robustness evaluation is accomplished using Shannon entropy, where the cryptographic reliability is evaluated. The hybridized THK-CSP-assisted CC privacy preservation is efficient due to the combination of exploitation and exploration capability. The performance of proposed technique is analysed through simulation to show the efficiency of functionality and the privacy-preserving mechanisms. Comparing to the state-of-art methods, the proposed THK-CSP for CC has highest Intrusion Detection Rate (IDR) of 97.456%. This goes to show that, when it comes to privacy and security, cloud systems are very efficient and come with high potency.

Keywords: *Privacy preservation, detection rate, optimization, HER, hash key, and cyber risks.*

Introduction

Privacy and security are two significant aspects which are crucial when it comes to the protection of Electronic Health Record (EHR) in the distributed cloud environments. As the dependency of organisations on cloud services to store and process their Electronic Health Record (EHR) increases, it becomes important to safeguard cloud ecosystems from threats and risks to guarantee the security of the organisation's information [1]. This paper encapsulates the challenges and opportunities which exist within the field of intrusion detection and privacy maintenance when it comes to distributed cloud based Electronic Health Record (EHR). IDS are important structures in the cloud security system because they provide a means of identifying and potentially threats and any access to the resources that is not allowed. As cloud computing environment is a distributed environment, it poses some issues for IDS such as scalability, dynamic management of resources and multi-tenancy. On the other hand, the traditional IDS models that was initially designed for closed on-premise networks can cause a number of problems when it comes to cloud environments, as the latter can be highly elastic and distributed.

To accommodate these challenges cloud-based IDS must be designed to work distributed over several nodes and virtual machines. These systems require constant scanning of the network traffic, the users' activities and the logs to look for signs of an intrusion. There has been a growing incorporation of the ML and AI techniques in cloud IDS with the aim of improving the detection rates [2]. These systems are trained on large volumes of normal and malicious activities and are thus able to detect patterns that indicate attack. However, the integration of ML and AI also brings the issues of the interpretability and the reliability of the detection outcomes, which is why the cloud security needs further research on the XAI.

Another important issue in the distributed cloud model is privacy preservation as due to shared infrastructures and multitenancy there are threats of data leakage between tenants. Data stored in cloud environment is also at risk of being compromised not only from external threats but also from internal threats such as the insiders and cloud service providers who have been compromised [3]. Data privacy can be achieved by employing proper means of data encryption, proper means of authentication and proper means of data anonymization. One of the most promising concepts among the techniques mentioned above is homomorphic encryption which enables to perform calculations on the encrypted data without decrypting it in advance. However, the computational overhead required for homomorphic encryption to be employed is still a hindrance especially for real-time applications [4].

Besides encryption, the privacy-preserving data mining (PPDM) is crucial in the cloud environment due to data accumulation in most cases. Some of these techniques include the differential privacy that guarantees it is practically impossible to reverse engineering and derive the original data from the outcomes. Intrusion detection and privacy preservation in distributed cloud environments are very essential as it helps in protecting data from unauthorized access. That is why, with development of cloud computing, the approaches to identify intrusions and protect privacy should be also changed [5]. Several methods have been introduced to enhance the system's features, including ML, AI, and homomorphic encryption, which are also considered to be promising solutions that come with new problems that need further study and development.

Research Motivation

The need for privacy preservation in cloud computing arises from the increasing threats to Electronic Health

Record (EHR) confidentiality and integrity in distributed cloud environments. Ensuring user trust and safeguarding sensitive information is paramount. The novel aspects of the proposed work include a new methodology to generate the Tiger Hash Key (THK) with the help of Goat Optimization Algorithm (GOA) incorporated for efficient intrusion detection and privacy maintenance. CSPs can be trusted by employing a trust model that is essential in enhancing security of Electronic Health Record (EHR) stored and processed in the cloud. Shannon entropy is used to evaluate the strength of the encryption so as to guarantee cryptographic strength. The proposed THK-GOA approach combines the exploitation and exploration capabilities of the system, thus improving the effectiveness and efficacy of privacy preservation in cloud computing. The simulations confirm that the performance is as intended, showing that the proposed method allows for functional preservation, and data protection. It also supports and enhances users' trust in cloud services due to changing privacy concerns and cybersecurity threats.

The remainder of the article is organised as follows: the overview of privacy preserving in cloud and intrusion detection along with research motivation is given in Section 1, the comprehensive analysis of recent literature with research gap is detailed in Section 2, the proposed Tiger Hash Key (THK) generation mechanism assisted Goat Optimisation Algorithm (GOA) security mechanism is detailed in Section 3, the simulation analysis with discussion is illustrated in Section 4, and the article is concluded with future enhancement in Section 5.

Related Works

In their work of Saravanan, V., et al. (2024) introduced the Blockchain-based African Buffalo (BbAB) with Recurrent Neural Network (RNN) model to detect intrusion more effectively. The normal and malware datasets are encrypted with help of Identity Based Encryption (IBE) and the encrypted data is stored in the blockchain. Intrusion is detected by the RNN and the African Buffalo optimization is used for real time intrusion monitoring. The model provides a high level of accuracy and recall of 99.87% and 99.92% recall for the cloud security indicating the efficiency of the proposed model [6].

In Manjushree, C. V., & Nandakumar, A. N. (2024) the Cloud Malware Intrusion Detection system using Harris Hawks Optimization (HHO) and Multilayer Perceptron (MLP) tackle malware threats in cloud computing. The MLP model identifies latent malware threats, improved for effectiveness by the HHO. The hybrid model means a 98.45% accuracy, 98.55% precision, 99.88% recall, and 99.21% F1 Score [7].] Duhayyim, M. A. , et al. (2022) propose a Stochastic Fractal Search Algorithm with Deep Learning Driven Intrusion Detection System (SFSA-DLIDS) for cloud-based cyber-physical systems (CPS). SFSA-DLIDS targets at intrusion detection based on min-max normalization, feature selection, and Chicken Swarm Optimization with Deep Stacked Auto Encoder which renders high security for CPS settings [8].

Ming et al. (2021) described as Single-Authority Attribute-Based Encryption (SA-ABE) The drawback is that only an attribute agency can assign user properties, so data can only be shared under the control of the attribute agency, and multiple attribute agencies cannot share data. MultiAgency Attribute-Based Encryption (MA-ABE), on the other hand, is better than SA-ABE. This not only meets complex access control and data confidentiality requirements but also allows data to be shared between permissions with different attributes. However, existing MA-ABE programs are not compatible with resource-restricted devices. This is because these programs are based on expensive pilot combinations. In addition, the main challenge of the MA-ABE program is the expiration of the properties [9].

Miao et al. (2021) described Searchable Encryption (SE) as an important technology that ensures the safety and availability of data simultaneously in the cloud. The Ciphertext Policy Attribute-Based Keyword Search (CP-ABKS) solution uses Ciphertext Policy Attribute-Based Encryption (CP-ABE) to simultaneously provide keyword-based acquisitions and sophisticated access control. CP-ABKS program, the task of single attribute permissions is to verify the validity of the user and the key distribution [10].

Wang et al. (2021) described, this challenge, the Recommendation System (RS) may invite a team of agents to collectively understand the user's preferences and preferences. This is called the Distributed Referral System (DRS). Agents need to share information to improve the accuracy of TRS traditional RS. However, due to a large number of candidates, it is difficult for DRS to provide customized recommendations for each user. In addition, sharing information between agents also brings with it privacy issues [11].

Qu et al. (2020) described as a large amount of data continues to be shared by various rapidly growing Cyber-Physical Social Networks (CPSN), privacy leaks become more and more serious. Differential privacy is one of the main ways to protect privacy, but most of its extensions assume that all data users share the same privacy requirements. Therefore, in reality, different privacy expectations cannot respond. Customization privacy protection based on different privacy may be a promising solution to this problem. However, that customizable security triggers a different privacy configuration mechanism, weakening privacy protection and causing unexpected interactions between input noises and leaking more important information [12].

The research gap lies in the absence of a comprehensive approach that addresses both privacy concerns and the efficiency of intrusion detection systems (IDS). While Saravanan, V., et al. (2024) propose a Blockchain-based scheme for enhanced intrusion detection, they do not specifically address the privacy challenges inherent in handling sensitive data. Hence, there's a need for innovative methodologies like the Privacy-Preserving Tiger Hash Key (THK) Generation Mechanism Assisted Goat Optimization Algorithm (GOA), which aims to rectify this issue by integrating privacy-preserving techniques with efficient optimization algorithms, ensuring both security and performance in IDS.

Proposed Methodology: Privacy-Preserving using Tiger Hash Key (THK) Generation Mechanism Assisted Goat Optimisation Algorithm (GOA)

In the privacy aspect, it is well maintained across the cloud as it is observed in the improvement of security issues as a chief concern. Here, the privacy concern and intrusion detection are improved by incorporating the proposed Goat Optimization Algorithm (GOA) assisted Tiger Hash Key (THK) generation mechanism. CPS performance is discussed in this section and the reliability of cryptographic approach is also justified. The above mentioned mechanism is described in detail in the following figure:

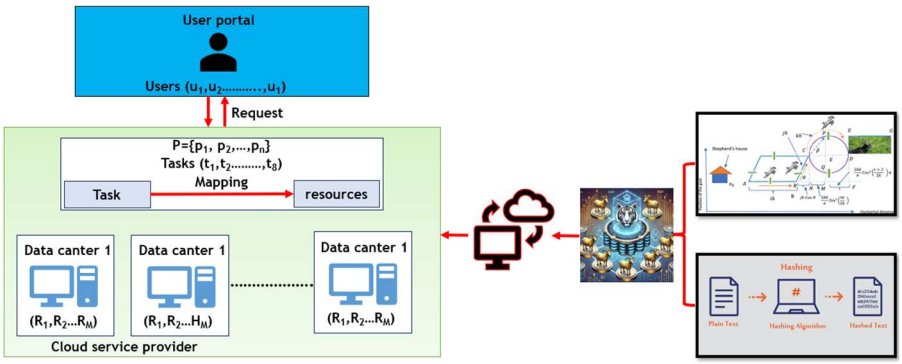

Figure 1. Goat Optimization Algorithm (GOA) assisted Tiger Hash Key (THK)

The presented research work enhances privacy and security of Electronic Health Record (EHR) in cloud computing through the provision of a new approach that integrates GOA with THK generation approach. This integration is intended to improve cryptographic security, intrusion detection and CSPs trust by optimization and hashing. This work combines the optimization affordance of GOA and the cryptographic security provided by the THK mechanism. The work which offers a novel solution is used to enhance the security of the cloud; it has great utility since it addresses two paramount issues of the cloud: privacy and computation.

Trust Model and Trust Score Calculation

The objective of the proposed trust model development is to come up with a measure of trust in the Cloud Service Provider (CSP). This is done by making a comparison of different trust indicators such as the performance history of the site, security, customer satisfaction and the reliability of the site. These parameters are then summed up to get a simple trust score, where MCDM technique is used where ever fuzzy logic or AHP is required. In the case of data collection, it entails the performance d Electronic Health Record (EHR) from the CSP logs in combination with the feedback from the users. This is followed by normalizing of the collected data so that the parameters are put in a single scale to enable comparison. The degree of trust is tied directly with the function of the weights assigned to each of parameters, which signifies how crucial they are in the process. Lastly, the overall trust is calculated by summing up the weighted parameters or else applying any other weighted sum aggregation function.

Let $P=\{p_1, p_2,\ldots,p_n\}$ be the set of trust parameters, where p_i represents a specific trust parameter. Let $w=\{w_1, w_2,\ldots,w_n\}$ be the set of weights associated with each parameter, such that $\sum_{i=1}^{n} w_i = 1$ and $0 \leq w_i \leq 1$.

Normalize each parameter p_i to a common scale, resulting in p_i'. Assign a weight w_i to each normalized parameter p_i'. Compute the overall trust score T using a weighted sum is given in Equation 1.

$$T = \sum_{i=1}^{n} w_i \cdot p_i' \text{---------(1)}$$

Entropy Calculation

The purpose of entropy calculation is to estimate the cryptographic security of the suggested key generation approach. This is done by testing the randomness and non-repeating nature of the generated keys since these are critical to achieving good cryptographic strength. This evaluation's data source includes key samples produced by the Tiger Hash Key (THK) mechanism. To measure the randomness, Shannon entropy is used. In this regard, each key is considered a random variable and the probability of each key is the frequency of occurrence of the key in the sample of keys. The entropy of the keys also increased, meaning that the keys are less predictable; thus, it would be difficult for attackers to deduce the pattern or sequences of the keys. On the other hand, smaller entropy values indicate that the string is more predictable and, therefore, less secure in terms of cryptography. Hence, when calculating the Shannon entropy of the generated keys it is possible to estimate the cryptographic reliability of the THK mechanism.

Given a set of key samples S, let $\{x_1,x_2,\ldots,x_n\}$ represent the unique keys in S. Let $p(x_i)$ be the probability of occurrence of key x_i, which can be estimated as the relative frequency of x_i in the dataset S.

Calculate the probability $p(x_i)$ of each unique key x_i is given in Equation 2.

$$p(x_i) = \frac{count(x_i)}{total\ number\ of\ keys\ in\ S} \text{---------(2)}$$

Compute the Shannon entropy H(X) for the key samples in Equation 3.

$$H(X) = -\sum_{i=1}^{n} p(x_i) log p(x_i) \text{---------(3)}$$

Goat Optimisation Algorithm (GOA) Assisted THK Generation

The Tiger Hash Key mechanism is improved by the parameters tuning of the Goat Optimization Algorithm (GOA) to achieve better cryptographic security and performance. GOA operates through exploration and exploitation phases: exploration helps to increase the area of search to avoid getting stuck at the local optimum while on the other hand exploitation helps in fine tuning the solution in the neighbourhood of the best configuration. This process of iteration proceeds until the solution is stabilized or the iteration limit has been attained. Hybridizing with THK depicts the benefits of a higher system performance as well as the enhancement of the protection of privacy in GOA. The THK algorithm, on its part, uses secure hash functions such as SHA-3 or Blake2 to guarantee the cryptographic security. This approach is quite effective in integrating the optimization of GOA with the firm cryptographic background of THK. Let M be the input data and divide M into n blocks of equal size b that is $M=\{B_1, B_2,\ldots,B_n\}$. Process each block B_i using the secure hash function H (SHA-3). Let h_i be the hash output of block B_i. Concatenate the hash outputs h_i to form an intermediate value I. Further hash the intermediate value I to produce the final hash value H_f.

The input division is given in Equation 4.

$$M = \{B_1, B_2, \dots\dots, B_n\}\text{---------(4)}$$

The block size is determined using Equation 5.

$$b = \frac{|M|}{n}\text{---------(5)}$$

The hash function is given in Equation 6 and the concatenation process is given in Equation 7.

$$h_i = H(B_i)\ for\ i = 1,2,3, \dots\dots, n\text{---------(6)}$$

$$I = \oplus_{i=1}^{n} h_i\text{---------(7)}$$

The iterative intermediate hashing is given in Equation 8.

$$I_j = H(h_1 \oplus \mathrm{h}_2)\text{---------(8)}$$

Final hash value is given in Equation 9 and iterative hash combination is given in Equation 10.

$$H_f = H(I_{n-1})\text{---------(9)}$$

$$I_j = H\left(I_{j-1} \oplus \mathrm{h_j}\right) for\ j = 2,3,4, \dots., n\ \text{---------(10)}$$

The process of padding is given in Equation 11.

$$If\ |M|\ mod\ \ b \neq 0, pad\ M\ to\ make\ it\ a\ multiple\ of\ b\text{---------(11)}$$

The Tiger Hash Key (THK) algorithm improves the cryptographic security since it uses secure hash functions such as SHA-3. Input data is then divided into blocks, hashed to produce outputs which are then concatenated to produce an intermediate value. This value is hashed, and the final value is reached after going through several hashing rounds thus making sure that even if the input is slightly different from the previous, the output will be very much different. Padding helps in balancing the Electronic Health Record (EHR) of different lengths to be processed to an equal level. To improve the privacy preservation of THK and make full use of the strong hashing

function of THK, THK's parameters are further optimized using the Goat Optimization Algorithm (GOA) in parallel with the THK framework.

The population size N is determined, maximum iterations k, and the initial population $G=\{g_1,g_2,\ldots,g_N\}$ and the THK parameter is determined by the vector g_i. The fitness function $f(g_i)$ is determined to evaluate each candidate solution g_i based on key strength and computational efficiency. The GOA is utilised to adjust the THK parameters to optimize the fitness function and it is calculated using the Equation 12.

$$f(g_i) = \alpha \cdot keystrength(g_i) + \beta \cdot computationalefficiency(g_i)\text{---------}(12)$$

where the weight factors are indicated using α and β.

The strength of the key is estimated using the Equation 13.

$$key_{strength}(g_i) = H(g_i)\text{---------}(13)$$

where the entropy function is indicated using H that evaluate the unpredictability and randomness of the keys generated.

The computational efficiency of proposed hybrid system is given in Equation 14.

$$Computational_{efficiency}(g_i) = \frac{1}{T(g_i)}\text{---------}(14)$$

where the parameter g_i is utilized for the processing and generation of keys whereas the time taken for that is indicated by $T(g_i)$.

The process of convergence attainment and the termination is given using Equation 15.

$$IF|f\left(g_{best}(t+1)\right) - f\left(g_{best}(t)\right)| < \in or\ t \geq k, stop\text{---------}(15)$$

where ϵ is a small threshold value for convergence, and k is the maximum number of iterations.

The integration of the Tiger Hash Key (THK) mechanism with the Goat Optimization Algorithm (GOA) is aimed at using the optimization feature of GOA to optimize the parameters of THK for better privacy preservation. This process starts with the creation of a population of goats; each goat is a potential configuration of THK parameters. In this way, the fitness of every configuration is estimated with a function that takes into account the key strength and the computational cost. Namely, specific strength is quantified by the entropy

function to guarantee the unpredictability of the key, whereas computational strength is inversely proportional to the time needed to generate and process the key. GOA performs exploration and exploitation steps in updating the positions of the goats in a successive manner. In exploration, goats are shifted in the solution space to prevent convergence to local optima while exploitation fine tunes the best solutions. Thus, in the proposed hybrid model, all the parameters of the THK mechanism are fine-tuned to achieve both high security and high efficiency of the model while maintaining privacy preservation.

Result and Discussion

The hardware and software simulation setup include a virtual computing environment with multiple GPU such as NVIDIA Tesla series for parallel computing. The server operates on a multi-core processor (for example, Intel Xeon) with not less than 128 GB RAM for processing big data and complicated crypto algorithms. It has an SSD-based storage system to ensure that there is easy access to data. The system implements the Goat Optimization Algorithm (GOA) using the Python programming language with libraries like TensorFlow or PyTorch. The Tiger Hash Key (THK) algorithm is created employing cryptographic libraries such as PyCryptodome. Calculations of entropy and network simulation is done using such tools as MATLAB. AWS or Azure is used to check the scalability and distributed computation in the cloud environment. Security metrics are collected by such tools as Wireshark, and specific IDS. To compare the proposed THK-CSP (Tiger Hash Key-Cloud Service Provider) methodology, the existing systems like, Blockchain-based African Buffalo (BbAB), and Harris Hawks Optimization and Multilayer Perceptron (HHO-MLP), Single-Authority Attribute-Based Encryption (SA-ABE), and Multi-Agency Attribute-Based Encryption (MA-ABE).

Latency is the time needed to compute and produce cryptographic keys such as the time for parameter optimization through the Goat Optimization Algorithm (GOA). Lower value is more desirable which means that the system can complete the encryption and decryption functions in a short amount of time, which is a crucial factor if the application is intended to run on the cloud in real time. Trust Score Accuracy (TSA) measures the reliability of the trust scores that are given to the CSPs in accordance to their performance, security, and customers feedbacks. It shows to what extent the trust model matches the real dependability and safety of each CSP and guarantees that data is processed by the most reliable contractors. Intrusion Detection Rate (IDR) on the other hand provides an idea of the system's ability to identify the intrusion attempts or possible security violations. A higher intrusion detection rate suggests that the system is better placed at detecting and preventing threats hence improving the security of the cloud environment. The performance is evaluated using the Equation 16 – 18.

$$L = T_{GOA} + T_{KeyGen} \text{---------(16)}$$

Where T_{GOA} is the time required for parameter optimization using the Goat Optimization Algorithm, and T_{KeyGen} is the time needed to generate the cryptographic keys. Lower latency indicates better performance.

$$TSA = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{|T_{pred}(i) - T_{actual}(i)|}{T_{actual}(i)}\right) \text{---------(17)}$$

Where $T_{pred}(i)$ is the predicted trust score for the i-th CSP, $T_{actual}(i)$ is the actual trust score, and N is the total number of CSPs. A lower TSA value indicates higher accuracy.

$$IDR = \frac{Count\ of\ Detected\ Intrusions}{Total\ Count\ of\ Intrusion\ Attempts} \times 100\text{---------}(18)$$

A higher IDR value indicates better detection capabilities, contributing to improved system security.

Table 1. Comparison of Latency (ms)

No of Users	BbAB	HHO-MLP	SA-ABE	MA-ABE	THK-CSP
200	567	548	531	489	389
400	589	571	539	498	399
600	599	581	542	523	411
800	609	593	550	545	423
1000	623	611	566	552	433

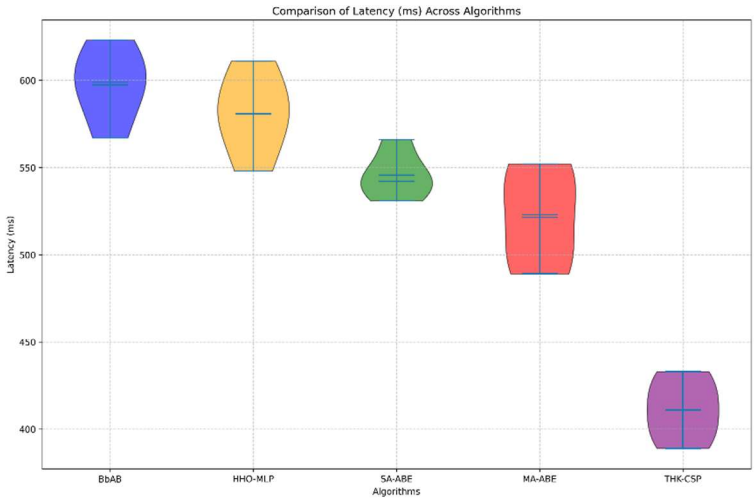

Figure 2. Comparison of Latency

The latency performance for the five algorithms BbAB, HHO-MLP, SA-ABE, MA-ABE, and THK-CSP are presented in Table 1 for different user counts. The latency values having the unit of milliseconds demonstrate that the THK-CSP algorithm has a higher performance compared to the other ones increasing the user number. For THK-CSP, the lowest latency is observed at 200 users with 389 ms, and such latency gradually rises to 433 ms at 1000 users. On the other hand, BbAB indicates the highest latency of 567 ms for 200 users and escalating to 623 ms, for 1000 users. As it is evident, the latencies of HHO-MLP, SA-ABE, and MA-ABE are moderate while the latencies of HHO-MLP and SA-ABE remain comparatively stable though less efficient than THK-CSP. The above results imply that, with more users, all algorithms for comparison have a scalable performance decrease in terms of latency, but THK-CSP is the least affected among all the tested algorithms, meaning that it is more suitable for applications that require low latency.

Figure 2 is the graphical representation of data presented in Table 1 in which the latency trends of the algorithms have been depicted. The latency curve is also clearly shown to belong to THK-CSP as the most efficient of the five as the curve is positioned under those of BbAB, HHO-MLP, SA-ABE, and MA-ABE. This graph highlights the advantage of THK-CSP in terms of scalability, as the curve it generates is much more shallow in comparison with the other algorithms, which exhibit much higher latency growth as more users are added to the system.

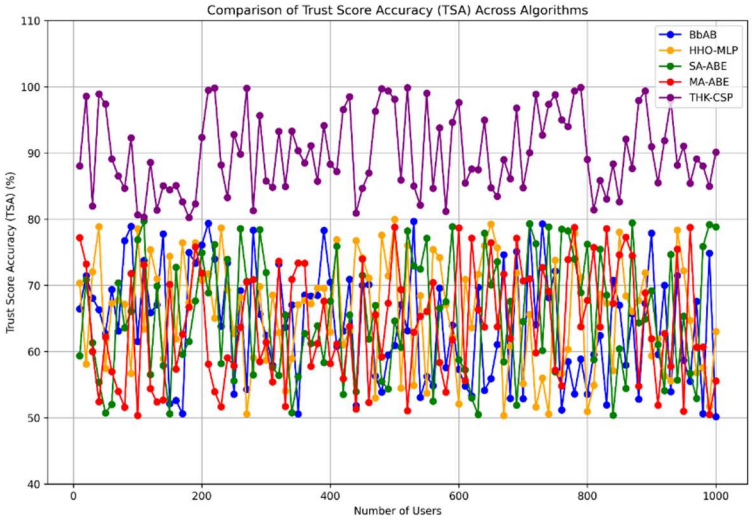

Figure 3. Comparison of Trust Score Accuracy (TSA)

The wave graph below depicts Trust Score Accuracy (TSA) of BbAB, HHO-MLP, SA-ABE, MA-ABE, and THK-CSP. THK-CSP also has the highest average TSA ranging from 80-100% for all the user intervals proving the hypothesis that it is a better system. On the other hand, BbAB and HHO-MLP have comparatively lower and constant TSA including SA-ABE and MA-ABE with an increase in the number of users that are still lower than THK-CSP.

Table 2. Intrusion Detection Rate (IDR) in %

No of Users	BbAB	HHO-MLP	SA-ABE	MA-ABE	THK-CSP
200	71.23	75	78.34	81.23	93.34
400	73.34	76.45	79.34	82.34	94.45
600	74.45	77.45	80.12	84.3	95.45
800	75.45	78.34	81.23	84.81	96.99
1000	76	79.12	83.03	85.34	97.456

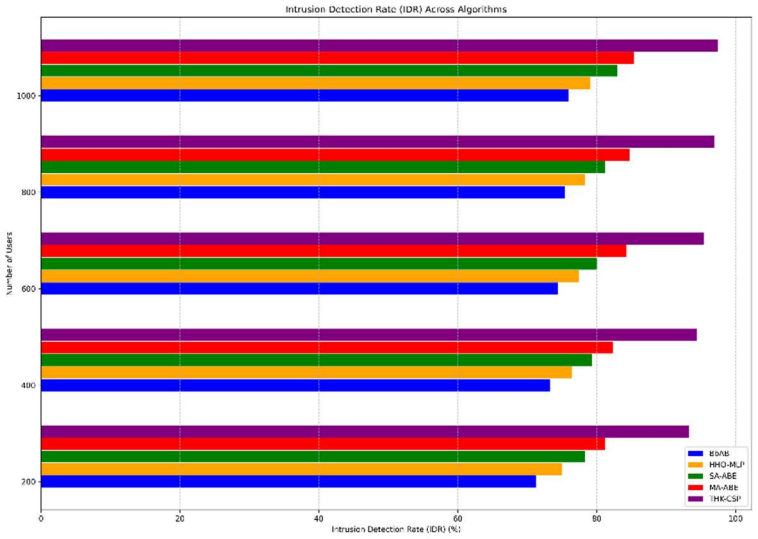

Figure 4. Intrusion Detection Rate (IDR)

Table 2 details the Intrusion Detection Rate (IDR) for the same algorithms. THK-CSP again leads, demonstrating the highest IDR across all user counts, reaching 97.46% at 1000 users. The other algorithms, while showing improvements in IDR as the user count increases, do not achieve the performance levels of THK-CSP. BbAB, with an IDR of 71.23% at 200 users, improves to 76% at 1000 users, but remains significantly behind THK-CSP. The sustained high-IDR of THK-CSP also supports the conclusion that it yields the best results in intrusion detection and thus is superior to all systems in the evaluated parameters. Figure 4 is a graphical presentation of IDR data that is shown in Table 3. The plot indicates that the proposed THK-CSP achieves better detection capabilities than the rest of the models, which can be observed from the fact that the IDR curve of THK-CSP always lies higher than that of BbAB, HHO-MLP, SA-ABE, and MA-ABE. This figure supports the tendency that the table demonstrates, proving THK-CSP's high performance and pointing out its ability to maintain high detection rates rising with the number of users.

The study results show that the GOA enhances the THK parameters that increases key unpredictability and better privacy preservation. This is manifested by high Shannon entropy values which are evidence of high cryptographic strength of the produced keys. Cyber-Physical Systems (CPS) performance is also improved since the proposed mechanism is reliable and efficient in providing security. For practical applications of real time cloud applications, the integration of GOA with THK has certain advantages to offer on the aspects of securing the application as well as improving the computational power. This makes the approach relevant for environments where high levels of data protection and privacy are necessary such as in cloud services. The work offers a solution with high scalability that can be applied to CSPs to increase the level of trust for customers through the better detection of intrusion and less vulnerability to security threats.

Conclusion

The THK generation mechanism introduced in this paper supplemented by the GOA will potentially contribute to the enhancement of intrusion detection and privacy preservation in the distributed cloud Electronic Health Record (EHR) system. This approach includes a more practical trust model coupled with sophisticated cryptographic methods in order to enhance the level of trust in CSPs. THK-GOA methodology is very cautious while evaluating the cryptographic reliability using Shannon entropy and ensures the resulting keys are unique and of high reliability. This strong key generation process is crucial because it contributes to the high protection level of Electronic Health Record (EHR), which is achieved due to the fact that these keys are relatively random and therefore can hardly be decrypted. This makes the THK parameters to be adjustable through GOA to new conditions and threats in order to enhance security functions of the AS. In total, one can state that the proposed THK-GOA approach is a rather effective solution for the enhancement of both privacy and security in the sphere of cloud computing to meet the modern challenges in IT concerning privacy preservation and trust. The subsequent work will be devoted to the enhancement on the scalability and generality of the THK-GOA mechanism.

The disadvantage of the proposed mechanism is that it suffers from the fact that large-scale systems will need substantial parameters tuning. However, the generalization of the approach might be a problem at a large and more complex infrastructure of the cloud. The future work may have to adjust the algorithm further to address these problems of scalability and expand these concepts to other contexts. Consequently, there are practical implications of the proposed THK mechanism with the help of the GOA that will provide better security and efficiency for real-time cloud application.

Reference

1. Ghosh, N., Ghosh, S. K., & Das, S. K. (2014). SelCSP: A framework to facilitate selection of cloud service providers. IEEE transactions on cloud computing, 3(1), 66-79.
2. Aruna, A., & Sellam, V. (2023, December). Security Framework for Electronic Health Record in the Cloud Based on Public key Encryption. In 2023 9th International Conference on Signal Processing and Communication (ICSC) (pp. 150-155). IEEE.
3. Raja, S. K. S., Sathya, A., Karthikeyan, S., & Janane, T. (2021). Multi cloud-based secure privacy preservation of hospital data in cloud computing. International Journal of Cloud Computing, 10(1-2), 101-111.

4. Hentschel, R., Leyh, C., & Petznick, A. (2018). Current cloud challenges in Germany: the perspective of cloud service providers. Journal of Cloud Computing, 7, 1-12.
5. Sathya, A., & Aruna, A. (2024). Rehabilitation for Parkinson's Disease Using Virtual Reality (VR): Impact and Observational Analysis. In Navigating the Augmented and Virtual Frontiers in Engineering (pp. 1-20). IGI Global.
6. Tharini, V. J., & Shivakumar, B. L. (2024). A Canonical Particle Swarm Optimization (C-PSO) Approach to Identify High Utility Itemset. Journal of Computational Analysis and Applications (JoCAAA), 33(05), 507-517.
7. Saravanan, V., Madiajagan, M., Rafee, S. M., Sanju, P., Rehman, T. B., & Pattanaik, B. (2024). IoT-based blockchain intrusion detection using optimized recurrent neural network. Multimedia Tools and Applications, 83(11), 31505-31526.
8. Manjushree, C. V., & Nandakumar, A. N. (2020). Dimensional Insight to Innovations in Security Aspects of Cloud Computing. In ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications (pp. 160-171). Springer Singapore.
9. Duhayyim, M. A., Alissa, K. A., Alrayes, F. S., Alotaibi, S. S., Tag El Din, E. M., Abdelmageed, A. A., ... & Motwakel, A. (2022). Evolutionary-based deep stacked autoencoder for intrusion detection in a cloud-based cyber-physical system. Applied Sciences, 12(14), 6875.
10. Ming, Y., He, B., & Wang, C. (2021). Efficient revocable multi-authority attribute-based encryption for cloud storage. IEEE Access, 9, 42593-42603.
11. Miao, Y., Deng, R. H., Liu, X., Choo, K. K. R., Wu, H., & Li, H. (2019). Multi-authority attribute-based keyword search over encrypted cloud data. IEEE Transactions on Dependable and Secure Computing, 18(4), 1667-1680.
12. Wang, S., Zhang, X., Wang, Y., & Ricci, F. (2022). Trustworthy recommender systems. ACM Transactions on Intelligent Systems and Technology.