Priyadarshini *et al.*
*Journal of Cloud Computing* (2022) 11:64
https://doi.org/10.1186/s13677-022-00336-z

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

# An enhanced encryption-based security framework in the CPS Cloud

R. Priyadarshini[1], Abdul Quadir Md[1*], N. Rajendran[2], V. Neelanarayanan[1] and H. Sabireen[1]

**Abstract**

The rapid advancement of computation techniques and cloud computing has led to substantial advancements in Cyber-Physical Systems (CPS), particularly in the field of health care. There are a variety of ways in which CPS is used in healthcare today, including delivering intelligent feedback systems, automatically updating patient data digitally, monitoring patients passively with biosensors, etc. In recent years, cyber-physical systems have become capable of making lifesaving decisions as they are becoming more connected to the cloud. However, healthcare has become one of the most critical issues for many. A CPS network uses the Internet of Medical Things (IoMT) to continuously monitor patients' health metrics such as body temperature, heart rate, etc. Due to physical connectivity restrictions, networks are more susceptible to security threats. In spite of the fact that the data is stored in the cloud, it is necessary to provide security regardless of device security and network security. Several cyber-security vulnerabilities have been identified in cloud-based healthcare systems in particular. To give patients a reliable healthcare experience, security concerns with CPSs need to be addressed carefully. In this context, this paper proposes a Cross-Breed Blowfish and MD5 (CBM) approach to improve the security of health data in the CPS cloud. The proposed model uses the wireless sensor network, in which data acquired by the network is transmitted via the transmitting node. Using the fuzzified effective trust-based routing protocol (FET-RP), the most efficient path for data travel is selected. The best route is determined using Butter-Ant Optimization (BAO) algorithm. The proposed method conveys data throughput encryption and decryption in a decoded format. The encrypted data is then stored in the cloud database for security reasons. The route finding algorithm is the one which is sending the data from one end to other end. The data is encrypted based on the source and destination. We compare the performance metrics of our recommended technique to those of other existing techniques, such as RSA, Two fish, ICC, and FHEA, in order to ensure that it performs optimally. The values of Cross Breed Blowfish and MD5 and FET-RP with regard to the performance metrics in terms of encryption (60 ms), decryption (55 ms), latency (60 s), throughput (97 mbps), security level (98%), and execution time (57 ms) which outperforms the conventional methods by 10–15%. Also the proposed encryption shows the considerable improvement in the level of security making our model a real world solution.

**Keywords:** Healthcare, IoMT, CPS, Cloud security, Encryption, CBM, BAO, FET-RP

## Introduction

Cyber-Physical Systems (CPSs) are large-scale, tightly interconnected, resource-constrained collections of dispersed cyber- and physical-system components. In CPS, the compute and communication cores keep tabs on, coordinate, and govern the physical systems and their operations [1]. Complex communication and processing activities required by mission-critical applications must be met with the restricted resources of all these physical components.

Therefore, these restrictions were removed once the idea of Service oriented architecture (SOA) was applied to "cloud-based computer systems (CPS)". As a result, the

*Correspondence: abdulquadir.md@vit.ac.in

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
Full list of author information is available at the end of the article

CPS benefits from enhanced interoperability, adaptability, and productivity [2].

According to the "National Institute of Standards and Technology (NIST), "a system environment that can rapidly build, modify, and provision auto-scale cyber-physical systems composed of a set of cloud computing based sensor, processing, control, and data services" best describes the "Cyber Physical Cloud Computing (CPCC)" architectural framework. This definition was published in 2013. Some of the most important functions performed by these systems include: 1) Smart Health, which includes medical devices and systems as well as automated pervasive health; 2) Smart Transportation, which includes air traffic control and intelligent transportation systems as well as unmanned aerial vehicles; 3) Smart Power Grid, which includes the electrical power grid as well as navigation and rescue applications; 4) Social Networking and Gaming. System security and privacy has become a pressing concern for CPCCS because of the importance of these many app many applications [3]. Several methods have been proposed in the literature for integrating service-oriented architecture (cloud computing) with CPS, with CPS seen as service models such as "platform as a service (PaaS) and infrastructure as a service (IaaS)" [4]. In addition, there really are application-specific methods, whereby technologies like the Cyber Physical System, Cloud Computing, and Wireless sensor networks are combined with more emphasis than security and privacy concerns are given. For this reason, we propose a safe service provisioning framework for CPCCS by drawing inspiration from the aforementioned methods, merging the aforementioned technologies (CPS, Cloud computing, and WSN), and also taking into account different security challenges associated to them [5]. The main contributions of this paper are as follows:

1. Using the FET-RP, the most efficient path for data transmission is determined.
2. BAO is used to find the optimal path.
3. CBM is used to convey the data throughout encryption and decryption in a decoded format.

A overview of the literature is described in Section II of this article. The suggested methods have been provided in section III. Results and comments are found in Section IV. The conclusion of the proposed study is summarized in Section V.

## Literature review

Sailer et al. [6] managed the security of the cloud platform and the hosted services, their approach is predicated on enhanced cooperation between cloud providers, providers, and consumers. It's based on many security protocols that facilitate the automation of security management. This proof-of-concept framework is live in a testbed cloud environment. By controlling the safety of a sample multitenant SaaS application, they were able to assess the framework's efficacy.

Mondal et al. [7] identify two issues with the security architecture and then offer two strategies to address them. The data's fundamental importance in safeguarding our CPS infrastructure from attack is addressed in the first recommendation, SCCAF (Smart Cloud Computing Adoption Framework). The second approach, in contrast, uses a modeled detector linked to physical nature to find node information.

Pacheco et al. [8] provide an IoT framework for developing reliable and protected IoT software and services. By providing a platform for developers, they can stop treating security as an afterthought and start thinking about it systematically across all IoT layers, with the functions and services provided at each level. They demonstrate the viability of our approach to protecting and securing IoT services in the cloud.

Haoxiang and Smys [9] introduced virtual machines (VMs) to host applications and the careful management of resources results in significantly reduced power usage in a cloud setting. Hrough this process of optimization, they are also able to address any concerns about the system's security and fulfill any QoS needs. The system's scheduling problem has been addressed via the use of a clever memory-aware scheduling technique and accompanying algorithm.

Sun and Shi [10] provide a model predictive control as a secure service (MPCaaSS) paradigm for cyber-physical systems (CPS) that may shield them from both internal and external disturbances. They begin by using a novel control parameterization based on Gaussian radial basis functions to create a double-layer controller architecture that can use cloud-edge computing. To assure the security of data packet transmission, they add an encoding scheme and an ECC-based encryption to the proposed MPCaaSS architecture as a second stage.

Verma et al. [11] explain that CPSs have been developed as a result of recent developments in information technology and the ever rising complexity of digital networks. A flexible and reliable architecture for carrying out analytics operations on massive data streams, such as processing, aggregating, and analyzing data at different granularities, is cloud-based analysis in CPS. A cyber-physical cloud computing system that combines heterogeneous networks with cloud computing is subject to a number of dangers.

Zhang et al. [12] look at the three computing paradigms described above as well as definitions of CPS before shedding fresh light on well-known frameworks.

They also conduct an analysis of the Cloud-Fog-Edge Computing application level in CPS and delve into a variety of methods and tactics to integrate big data applications into a more advanced and practical society while addressing present shortcomings.

Kumar et al. [13] discussed that virtual machines (VMs) are used in the cloud environment for hosting applications and managing resources to optimize energy usage. Optimizing the system architecture also addresses security concerns and the quality of service (QoS) demands of the system. The use of a productive memory-aware scheduling approach and algorithms addresses the system's scheduling problem. The effectiveness of the suggested method is evaluated, and the simulation's findings are reported.

For CPSs, the model of predictive control as a secure service (MPCaaSS) framework is proposed by Trivedi et al. [14] to deal with both online threats and external interruptions. A novel control parameterization based on Gaussian radial basis functions, we construct double-layer controller architecture to benefit from cloud-edge computing. The controller settings and status measurements may then be encrypted, preventing hostile attackers from tampering with the communication and corrupting it.

Rahman et al. [15] presented framework replaces the long-standing certificate authority after strengthening the consortium block chain, which shortens the time it takes to process data and boosts throughput at a reasonable price. However, the distributed Industry 4.0 security paradigm calls for cooperative trust as opposed to relying on a single party, effectively accommodating the costs and risk of the single point of failure.

Bagheri et al. [16] provided a secure, federated architecture for training prognostic and diagnostic models without any data exchange. The suggested architecture ensures data privacy while producing thorough models that take advantage of the various activities of many organizations.

Wang et al. [17] provided a summary of the CPS security research over the last 5 years and choose 142 relevant works from conferences and publications of A- or B-level that the China Computer Federation has approved. First, they analyze the primary points of the chosen articles and group them into 24 categories. Then, they examined CPS security technology hotspots and trends from three angles: application scenarios; architectural layers (perception, network, and application); and MADC (Measure, Attack, Defense, and Control) kinds.

Kaur et al. [18] explain CPS combines networks, calculations, and physical processes to govern operations, react to changes in the environment, provide feedback, and adapt in real time. Disruptive CPS challenges governed by IoTs and IoE, integration with machine learning functions, cloud computing, and rising yet difficult focus on the core areas of Big Data Analytics, Virtualization, and Automation are all obstacles to Industry 4.0 success.

Egala et al. [19] address the shortcomings of block chain-based cloud-centric IoMT healthcare systems, such as excessive latency, high storage costs, and single points of failure, we have presented the hybrid computing paradigm with the distributed data storage system based on block chain. To enhance the proposed system's security, a decentralized selective ring-based access control mechanism, device authentication, and patient record anonymization methods are also provided. On the suggested system employing Block chain, we have assessed the latency and cost-effectiveness of data exchange.

## Materials and methods

In this section, we explain about the security framework in CPS cloud. Figure 1 depicts the framework for the proposed method. The novelty of the proposed method is that encryption is enhanced with cross breed technique and the optimization is performed using BAO optimization. The collected data is relayed through the transmitting node once the Wireless Sensor Network (WSN) has been installed. The fuzzified effective trust-based routing protocol (FET-RP) selects the most effective route for data to transit between two points. The optimal path is chosen using the Butter-Ant Optimization (BAO) approach. Even though, there are many optimization algorithms such as genetic algorithms, machine learning algorithms and other algorithms like Swarm particle, Ant colony optimization are famous nad gives maximum results. The suggested approach is used to transmit the data during encryption and decryption in a decoded format. The encrypted data are then stored in the cloud database for security purposes.

To train and assess the illness, data from the "UCI machine learning repository, Framingham, and Public Health Dataset" were used. The system uses three publicly accessible online datasets for cardiac disease: the "Framingham, Public Health, and Hungarian" databases. There are around 76 properties in this database, however only a subset of 14 features, as indicated in the table, were used in published study. Table 1 indicates the dataset description.

### Fuzzified effective trust-based routing protocol for low-power, Lossy network (FET-RPL)

#### *IoT effective fuzzy trust model*

A multi-step fuzzy component is used to determine trust. To assess trust for each trust dimension individually in the first step, fuzzy logic is used. Next, fuzzy logic is used

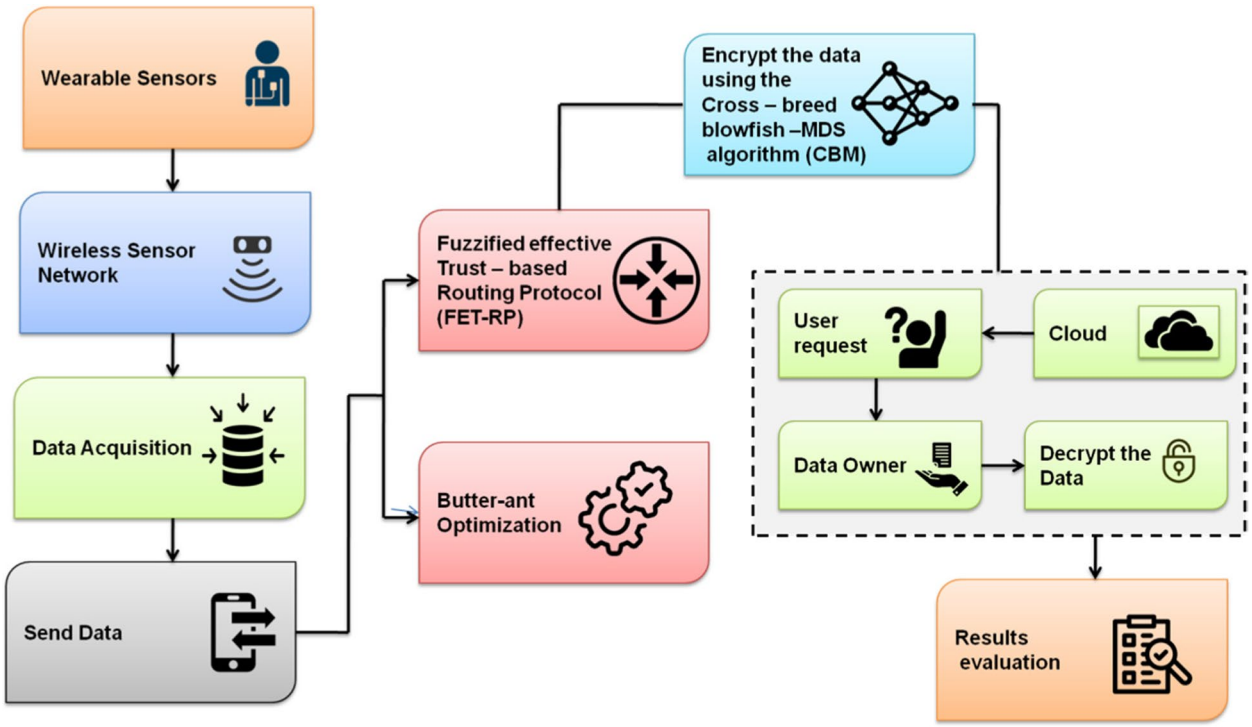


**Fig. 1** Framework for butter-ant optimization method

to calculate the greatest level of confidence. The whole dynamical fuzzy logic-based notion is implemented a secure "routing protocol for low-power and lossy network (RPL)". The FETM-IoT is a multi-level fuzzy model for determining if IoT devices can be trusted. Three dimensions are used in the FETM-IoT first fuzzy stage to assess reliability. Contextual data, QoS, and P2P communication quality (QPC) are all considered. Because dimensions and evaluation methods were carefully considered, the model is dynamic and comprehensive. The FETM-IoT project has a hierarchical structure. As can be seen below, each dimension therefore has its own sub-dimensions. This framework may be used to build a dynamic model.

This dynamic model may easily have additional dimensions and sub-dimensions added or deleted. Systems for FI are put out for every dimension individually. The "fuzzy inference (FI)" system is supplied into the final fuzzy system in all dimensions during the second stage of FI [20]. This inference technique enables the determination of a final degree of confidence.

### *FET-IoT-based routing protocol for low-power, Lossy network (FET-RPL)*

The FET-RPL, which enables secure interoperability, is composed of four fundamental processes. This cooperative strategy may be used to provide secure and dependable routing information to IoT devices. In-depth descriptions of the FET-RPL process are provided in the following sections.

The FET-RPL fuzzy trust model may be used in a "low-power, lossy network" to evaluate trust between entities. Two stages make up the "FET-RPL".

First, 3 dimensions are taken into account. QoS, QPC, and contextual data are all significant [21]. Each of the four dimensions has a unique fuzzy system. The fuzzy system's second stage uses the outputs from the first fuzzy stage as inputs. The degree of trust between B and C is ultimately determined by the second phase. Given that it takes into account dimensions and computation methods, FET-RPL is a continuous and comprehensive model. Having access to active and ongoing advice is another aid in modeling dynamism. For behavior to adapt to the background, both direct and indirect information must be taken into consideration. The fuzzy location zone may be indicated using the radius$u_{18}$ as an example.

$$u_{18} = v_{18} * x_{max} \tag{1}$$

The fuzzified is used in FI systems to assess fuzzy set membership. A membership function calculates each fuzzy set in a fuzzified. This created a fuzzy set with three membership functions.

**Table 1** Dataset description

| Attribute | Description |
|---|---|
| Age | Age in years |
| sex | Sex (1 = male, 0 = female |
| ca | Number of major vessels (0–3) colored by flourosopy |
| fbs | Fasting blood sugar > 120 mg/dl) (1 = true; 0 = false) |
| oldpeak | ST depression induced by exercise relative to rest |
| chol | Serum cholestrol in mg/dl |
| num | Diagnosis of heart disease (angiographic disease status)<br>0. absence (< 50% diameter narrowing)<br>1–4. Present of heart disease (> 50% diameter narrowing) |
| slope | The slope of the peak exercise ST segment<br>1. upsloping<br>2. flat<br>3. downsloping |
| thalach | Maximum heart rate achieved |
| restecg | Resting electro cardio graphic results<br>0. normal<br>1. having ST-T wave abnormality (T wave<br>Inventions and/or ST elevation or<br>Depression of > 0.05 mV<br>2. showing probable or definite left<br>Ventricular hypertrophy by Estes' Criteria |
| exang | Exercise induced angina (1 = yes; 0 = no) |
| trestbps | Resting blood pressure (in mm Hg on admission to the hospital) |
| cp | Chest pain type<br>1. typical angina<br>2. atypical angina<br>3. non-anginal pain<br>4. asymtomatic |
| thal | 3 = normal; 6 = fixed defect; 7 = reversable defect |

$$f_{\mu}(z) = \frac{1}{\sqrt{2\pi\sigma}} f^{-\left(\frac{(z-\mu)^2}{2\sigma^2}\right)} \tag{2}$$

$$\begin{cases} f_{low}(z) = \frac{1}{\sqrt{2\pi}\times 0.3} h^{-\left(\frac{(z-0.2)^2}{2\times(0.3)^2}\right)} \\ f_{medium}(z) = \frac{1}{\sqrt{2\pi}\times 0.3} h^{-\left(\frac{(z-0.5)^2}{2\times(0.3)^2}\right)} \\ f_{high}(z) = \frac{1}{\sqrt{2\pi}\times 0.3} h^{-\left(\frac{(z-0.8)^2}{2\times(0.3)^2}\right)} \end{cases} \tag{3}$$

In the RPL topology, each node establishes connections with its neighbours and sends information at a power level that is appropriate for its transmission range. Consequently, e is the communication range.

$$F_j^{mt} = m * \left(F_{elec} + F_{amp} * f^2\right) \tag{4}$$

$$F_j^{mr} = m * F_{elec} \tag{5}$$

RPL will be enhanced by trust-based routing. A number of trust metrics have been added to this protocol to make routing decisions safer. The routing protocol known as "RP-LLN", or "routing protocols for low-power and lossy networks", is by far the most used. RPL makes use of a distance vectors routing technique to prevent network loops. Despite the fact that it works well in "P2MP and MPP" communication modes, RPL does not permit point-to-point communications. Any application may be tailored to meet RPL by using the appropriate routing metrics. Many applications could run badly as a result of the general features of RPL's lack of fine-tuning. Using the butter Ant optimization algorithm (BAOA), the performance of the FET-RPL is optimized.

#### Butter ant optimization algorithm

According to the butter ant (BA), the fitness of each BA optimization in the BAOA algorithm varies. Each BA enhances the process along by exuding a distinct aroma according on the degree of its fitness, which helps the optimization process even more. Butterflies may communicate with one another by exhaling a fragrance that is picked up by the environment.

A BA optimization follows other optimizations because it can follow the fragrance of other BAs. One BA optimization will grab attention to itself if its scent is greater than the others'. As a result, each BA moves at random in the direction of the one with the strongest scent. The geography of the target function influences or dictates the BA optimization's stimulus intensity. The BAOA algorithm has three essential phases: startup, iteration, and finalisation. The start-up process is carried out as normal each time BAOA turns on. Once the best response has been found, the process of searching is finished. This stage in algorithm development establishes the goal function and solution space. The values for the variables used in BAOA have been assigned. Once the settings have been specified, the algorithm generates butter-ant populations. A certain amount of Memory is made available for the butter-ant data during the BAOA simulations. The fragrance and fitness values of Butterant are calculated, recorded, and then their locations in the search space are generated at random. After completing this phase, the algorithm continues on repetation, which searches using the freshly created fake butter-ant. Every time the second phase of the BAOA is repeated, the performance values of every BA are computed and assessed. The butterflies then utilise the following formula to create scent:

$$f = dK^c \tag{6}$$

No other BAs can detect the smell that one BA is emitting when the value of ant is 0. Therefore, by adjusting the

value of the BAOA's power exponent, one may affect the BAOA's behaviour. These two parameters, as well as the sensory modality value, have a significant impact on the algorithm's convergence rate. The sensory modality (u) value in the BAOA is changed as follows:

$$d(q) = \left[ d(q-1) + \frac{0.025}{d(q-1) * Q} \right] \tag{7}$$

There is a broad range of absorption rates according on the sensory modality, which influences the power exponent. Argument f contains the scent value,where "d stands for the sensory modality" and K for the stimulus intensity. The values of parameters c and d, which have values between [0, 1], have an impact on the performance of algorithms.

$$z_k^{q+1} = z_k^q + \left( t^2 \times i^* - z_k^q \right) \times f_k \tag{8}$$

Where, $z_k^q$ stands for the butter-ant in the $j^{th}$ iteration. Additionally, $i^*$ is the leading BA in the iteration, $f_k$ is $j^{th}$ butterfly's fragrance, and t is a number drawn at random between 0 and 1. With this technique, the following may be done for local searches:

$$z_k^{q+1} = z_k^q + \left( t^2 \times z_j^q - z_m^q \right) \times f_k \tag{9}$$

In where $z_j^q$ and $z_m^q$ are the $m^{th}$ and $m^{th}$ BA in the same swarm, and t is a random value between 0 and 1.

Using forward and backward ant movements, BA is employed in this approach to discover the best route to the desired Location. The calculation of the network's maximum number of pathways max $NV_{yz}$ is specified by

$$\max\_NV_{yz} = \frac{LL_{yz}}{L_w + \Delta L} NL_{yz} \tag{10}$$

The following criteria are used to calculate the density of path ($D_{yz}$):

$$D_{yz} = \frac{NV_{yz}}{\max\_NV_{yz}} \tag{11}$$

Equations 11, 12 relate to find the density of the path and the butter ant optimization technique is related to the route finding and optimization with encryption, thus it is related.

Butter-ant optimization uses forward butter-ants to find the quickest and optimal path to the destination. The advance ants describe the migration of a new location as follows:

$$u_{yz}^m(q) = \begin{cases} \frac{c(\partial_{yz}) + b(1-\eta_{yz})}{\sum_{h \notin qcbv_m} c(\partial_{yz}) + b(1-\eta_{yz})} \times \left( \frac{1}{1+\frac{1}{N_j}} \right) \\ 0 \\ if\ j \notin qcbv_m \end{cases} \tag{12}$$

$\partial_{yz}$ - the pheromones values of an BA at ynode to portable to z node is denoted and is calculated backwards by BA, $\eta_{yz}$ - represents a vehicle's assessment of some fuzzy values on the link from y to z, c replicates the significance of $\partial_{yz}$ in terms of its weight, and b shows the relevance of $\eta_{yz}$ weight in the equation. An ant in motion becomes a backward one when they reach their destination, and vice versa. For this reason, inferior BA use the memories of their superior counterparts to select the optimum path.

**BAOA PSEUDO-CODE**

**Input: t, f, n, and q; Output: i***
Initiate the probability switch (t), Power exponent (f)
Mode of perception (n), and population size of BA(q).
Set s = 0
for (K = 1:K < =n) do
Make a tiny BA starter colony.
Find the fitness levels of every BA.
Calculate the fragrance of the BA using the eq. (9).
Choose the BA that will provide the best total solution (h*)
stop for
Although not being met, the stop requirements (s < n) do
Set s = s + 1.
for (K = 1:K < =n) do
Generate a random number d, d ϵ (0,1)
if (u < t) then,
Check to see whetherBA is at its best (i*) as in equ. (10).
Otherwise
Move the BA at random, as in eq. (11).
When end-if
Every BA is assessed according to its fitness function.
stop for
choose the finest solution for the each and every situation (i*)
Determine the value of the sensory modality using equ. (12).
stop
Generate the better solution (i*)

## Encrypt the data using cross breed blowfish- MD5 algorithm (CBM)

In order to increase security, this study suggests a novel parallel cryptographic method that combines and modifies the MD5 and Blowfish encryption algorithms. Figure 1 shows the schematic diagram for the suggested technique. The analysis and storage indicates the cloud storage and the methodology carried out in cloud for various process in the framework (Fig. 2).

### *Blowfish algorithm*

With a variety of parameters ("key size, square size, number of rounds") that may be used to balance safe quality with power consumption and computational overhead, Blowfish's cryptographic calculation is highly efficient and customizable. This blowfish calculation could function well with different data amounts under the right circumstances. When compared to algorithms, the blowfish computation had a favorable impact on the cryptography industry. The author also suggested a multifunctional

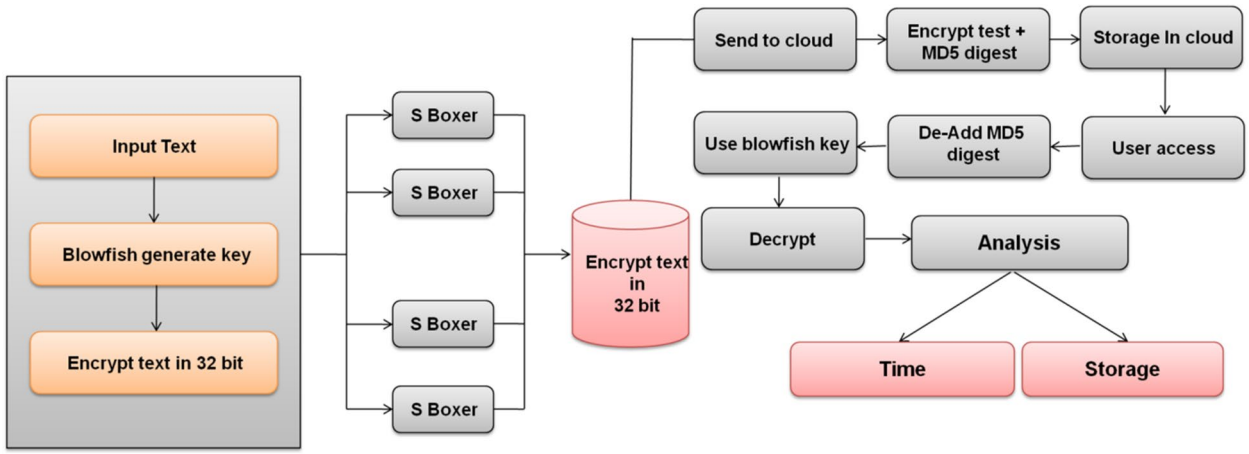


**Fig. 2** Cross-breed blow-fish based framework

security system that links the physical and logical worlds via near field communication and employs remote sensor organisers for data and vaccine security.

**PSEUDOCODE FOR BLOWFISH**

**Input: (64-bit), Y as the text.**
**Output: Encrypted data**
In the text, there are two 32-bit halves: $Y_M$ and $Y_S$
For J = 1 to 16:
$Y_M = Y_M$XOR QJ
$Y_S = G(Y_M)$ XOR$Y_S$
$Y_M$ and $Y_S$ is switched
Next J
Again $Y_M$ and YS is switched (Last switch undo)
$Y_S = Y_S$ XOR $Q_{17}$
$Y_M = Y_M$ XOR $Q_{18}$
Combined $Y_M$ and $Y_S$
Compute Function f:
$Y_M$ is split into four eight-bit quarters: B, C, D, and E $f(Y_M) = ((T_1, B + T_2, C$ mod 232) XOR $T_3$, D) + $T_4$, E mod 232
**Decryption:**
Instead, the decryption is similar, except the inverse order of $Q_1, Q_2 \ldots$ $\ldots \ldots . Q_{18}$ is used.
**Generation key:**
Initiated Y boxes and Q arrays
The 32 key bits of the first Q array are XOR'd with the 32 key bits of the second Q array, and so on.
The approach described above is used to encrypt all zero strings.
new input is provided by $Q_1$ and $Q_2$
With the use of sub-keys, a completely new $Q_1$ and $Q_2$ have been encrypted.
$Q_3$ and $Q_4$ are the newly generated outputs.
Repeating this method 512 times yields a fresh Q-array and four S-boxes to be calculated.

### *MD5 algorithm*

An MD5 message is composed of sixteen 32-bit sub-blocks that are separated by 512 bits each (Message-Digest algorithm). The 128-bit message processing of MD5 uses four linked 32-bit barriers to demonstrate honesty. This MD5 hash generator is useful for encoding passwords and also in encryption of the data. The very same purpose its used in the proposed study too.

**PSEUDOCODE FOR MD5**

**Input: (64-bit)**
**Output: Encrypted data**
The no. of input bits is verified.
A process of adding additional bits to messaging input such that the total data size is equivalent to 512 multiples
m is the result of adding 64-bit MI to the output of step 2.
The blocks from m to b are separated (512 bit each).
This is a list of blocks, each with 32 bits, from b to x (16).
The algorithm has four rounds, each with 16 steps (total is sixty four step).
There are four hex-encoded shift registers, each with a capacity of 32 bits.
regb = [7 6 5 4 3 2 1 0]32- bits [b]= [e]′
reg c = [g f e d 8 b 9 7] 32- bits [c]= [d]′
reg d = [8 9 b c d e f h]32- bits [d]= [e]′
reg e = [0 1 2 3 4 5 6 7]32-bits [e]= [b]′
bb, cc, dd, &ee are used to temporarily store the b, c, and d values.
Several variables g, h, i, and J are involved in the algorithm processing.
Shown below is a one-step operation:
b = c + ((b + f(c, d, e) + $y_j$ [l] + u [j] <<< T
where
$y_j$ [l] ← is the 32 bit $l^{th}$ word of $y_j$
<< <T←left circular shift of S bits
After every round's final output is added, the first round's input is used as the output.
The output bit depth is increased to 128 bits

### *Key generation and authentication*

As soon as the patient registers, a doctor will be assigned to them. For the initial password-based validation, both doctors and patients employ a secure password (MD5)-based technique. The technology compares the doctor's palm/thumb photo scan reading to the recorded data when the doctor checks in to see patient data. After a doctor's identify has been confirmed, access to the

system will be granted. For security purposes, a biological key is made from the patient's palm or thumb.

### *Decryption*

After extracting an authentication code or frame value from the previously constructed frame and completing the whole technique for constructing an authentication code as provided, authentication will be completed. Only then will decryption start. The patient's data, which consists of a group of sensors and a control unit, is kept in an encrypted form. If data consumers possess the set of decryption characteristics specified by the signature access structure, they may verify the authenticity of the cypher text and decode the data.

## Experimental results and discussion

In this section, we study the security framework in CPS cloud and compare the performance of our suggested technique to that of other existing methods. The existing methods are RSA [22], Twofish algorithm [23], improved chacha20 algorithm (ICC [24]), Fully Homomorphic encryption algorithm (FHEA [25]).

Encryption time analyses and illustrates the average amount of time required to encrypt media content files as input. The duration is measured in milliseconds (ms). Figure 3 and Table 2 shows the Comparative evaluation of Encryption time in Suggested and Traditional Methods.

When compared to the current techniques RSA, Twofish, ICC, and FHEA, which have encryption times of 90 ms, 84 ms, 70 ms, and67ms, respectively, the suggested CBM takes just 60 ms.

**Table 2** Comparative evaluation of encryption time

| Methods | Encryption time (ms) |
|---|---|
| RSA [22] | 90 |
| Twofish Algorithm [23] | 84 |
| ICC [24] | 70 |
| FHEA [25] | 67 |
| CBM [Proposed] | 60 |

Therefore, when compared to current techniques like RSA, Twofish, ICC, and FHEA, the CBM enhances security [26].

Decryption is the process [27] of converting a encrypt data back to its original state. Reverse encryption is a widely used technique. Only authorised persons are able to access encrypted data because decryption needs a hidden key or password. Figure 4 and Table 3 shows the Comparative evaluation of decryption time in Suggested and Traditional Methods [28]. When compared to current techniques RSA, Twofish, ICC, and FHEA, which have decryption times of 98 ms, 84 ms, 78 ms, and67ms, respectively, the suggested CBM takes 55 ms. Therefore, when compared to current techniques like RSA, Twofish, ICC, and FHEA, the CBM enhances security.

The amount of time that elapses between the moment that a user submits a request and the time that the server

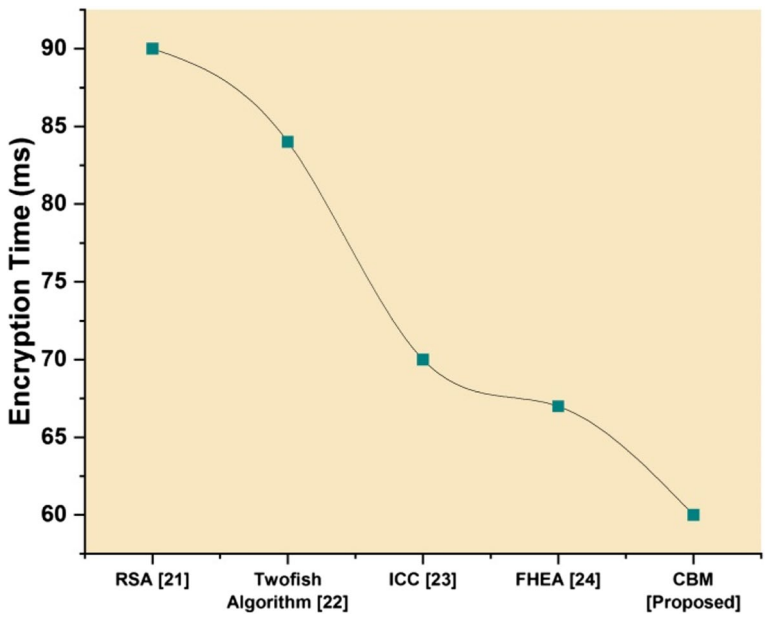


**Fig. 3** Comparative evaluation of encryption time

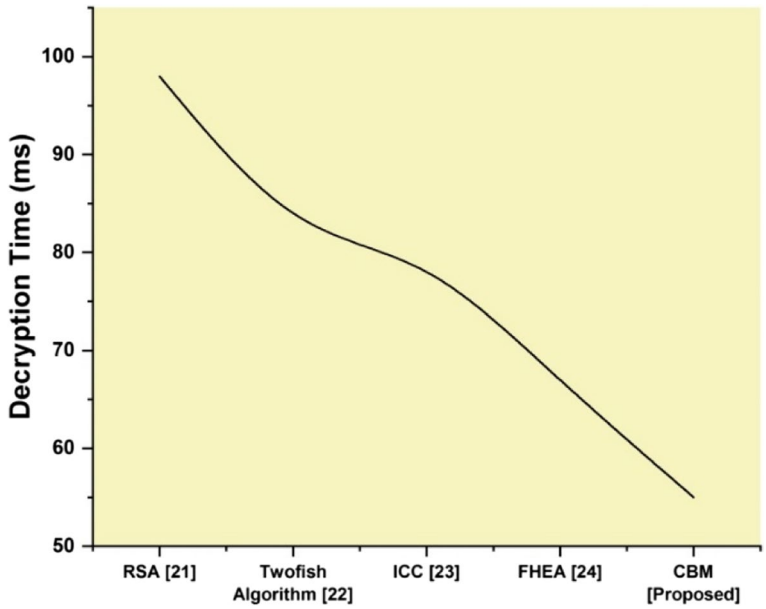


**Fig. 4** Comparative evaluation of decryption time

**Table 3** Comparative evaluation of decryption time

| Methods | Decryption time (ms) |
|---|---|
| RSA [22] | 98 |
| Twofish Algorithm [23] | 84 |
| ICC [24] | 78 |
| FHEA [25] | 67 |
| CBM [Proposed] | 55 |

returns a response is known as latency. It is measured in seconds. Figure 5 and Table 4 shows the latency. When compared to the current techniques RSA, Twofish, ICC, and FHEA, which have latency of 58 ms, 65 ms, 70 ms, and85ms, respectively, the suggested CBM takes 97 ms. CBM proposed latency was implemented in less time than existing methods such as RSA, Twofish, ICC, and FHEA.

The calculation of the risk that a security event will be attempted or occur is known as the security level.

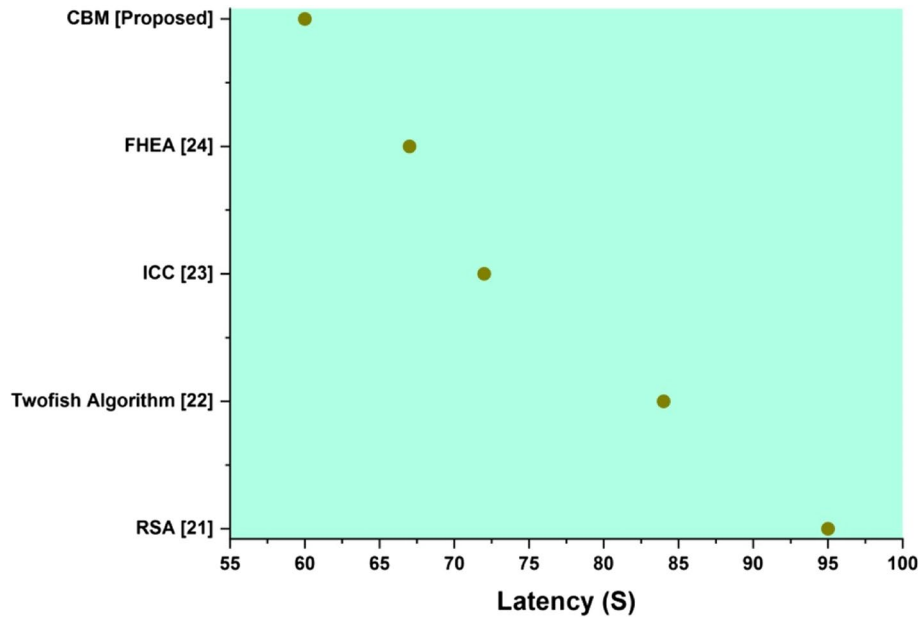


**Fig. 5** Comparative evaluation of latency

**Table 4** Comparative evaluation of latency

| Methods | Latency (s) |
|---|---|
| RSA [22] | 95 |
| Twofish Algorithm [23] | 84 |
| ICC [24] | 72 |
| FHEA [25] | 67 |
| CBM [Proposed] | 60 |

The results show that the proposed method CBM has high degree of security than existing methods such as RSA, Twofish, ICC, and FHEA.

The quantity of information a system can process or transmit in a given length of time is known as Throughput. The quantity of data that the users get from the server at any given second is measured in Megabytes per second (Mbps). Figure 7 depicts Comparative analysis of throughput in Suggested and Traditional Methods.

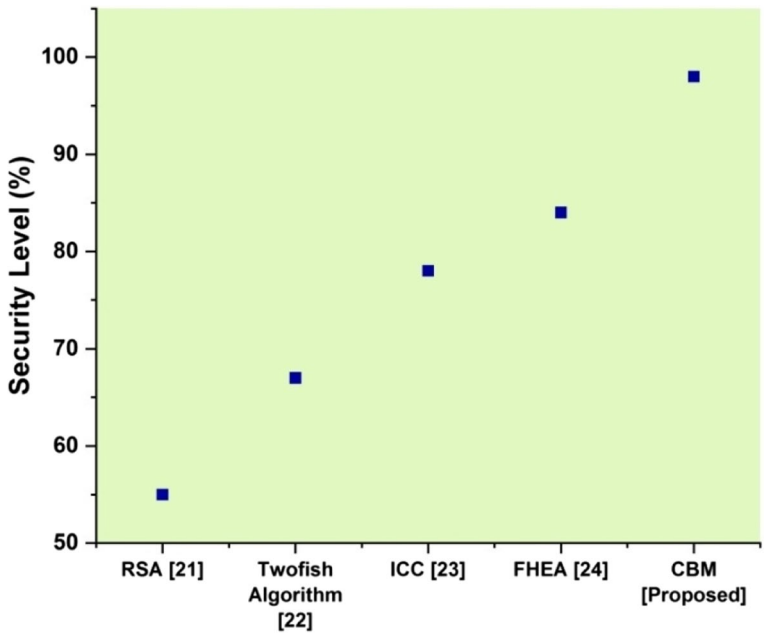


**Fig. 6** Comparative evaluation of security level

**Table 5** Comparative evaluation of security level

| Methods | Security level (%) |
|---|---|
| RSA [22] | 55 |
| Twofish Algorithm [23] | 67 |
| ICC [24] | 78 |
| FHEA [25] | 84 |
| CBM [Proposed] | 90 |

Figure 6 and Table 5 shows Comparative analysis of security level in Suggested and Traditional Methods. When compared to the current techniques RSA, Twofish, ICC, and FHEA, which have latency of 55%, 67%, 78%, and-84percent, respectively, the suggested CBM takes 98%. When compared to the current techniques RSA, Twofish, ICC, and FHEA, which have throughput of 58 Mbps, 65 Mbps, 70 Mbps, and85 Mbps, respectively, the suggested CBM takes 97 Mbps. To transmit or process information using proposed method CBM has high efficiency than existing methods such as RSA, Twofish, ICC, and FHEA (Table 6).

When estimating the execution time of a task, the amount of time the system spends performing run-time or system actions on its behalf is taken into consideration. The method for estimating execution time depends on the implementation. It is measured in milliseconds(s). Figure 8 depicts the Comparative evaluation of execution time in Suggested and Traditional Methods.

The execution time in RSA, Twofish, ICC, and FHEAare97 ms, 84 ms, 71 ms, and 64 ms respectively.

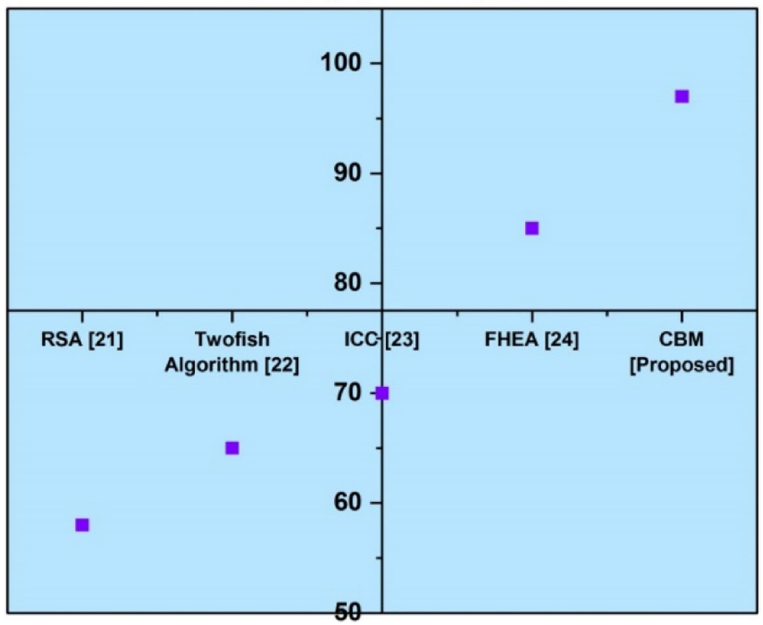


**Fig. 7** Comparative evaluation of throughput

**Table 6** Comparative evaluation of throughput

| Methods | Throughput (Mbps) |
|---|---|
| RSA [22] | 58 |
| Twofish Algorithm [23] | 65 |
| ICC [24] | 70 |
| FHEA [25] | 85 |
| CBM [Proposed] | 97 |

The execution time in proposed CBM is 57 ms.As performance results show that the execution time of CBM is also lower than the other existing. In conclusion, the CBM method outperforms than the RSA, Twofish, ICC, and FHEA in terms of execution time (Table 7).

## Discussion

RSA only employs symmetric encryption and full encryption requires the use of both symmetric and asymmetric encryption, it may sometimes fail [22]. Larger encrypted data makes two fish safe. This big size may slow down the application if it's applied to significant amounts of unencrypted data [23]. Slower encryption speed as encryption and decryption both require capturing the complete block. ICC is prone to mistakes as well since a mistake in a single symbol might change the whole block [24]. FHEA implies that data processing may be delegated to a third party without having to have faith in the security of the data. It is impossible to retrieve the original data without the correct decryption key [25].

## Conclusions and future work

The CPS Cloud protects the data's integrity and privacy while enhancing security. Our paper investigates the CBM approach to improve the security of health data in the CPS cloud. In a wireless sensor network (WSN) [29], connected wearable devices collect healthcare data, and that data is sent to a sending node [30]. A fuzzified effective trust-based routing protocol (FET-RP) selects the data route that will transmit the most data efficiently. To find the optimum path, the Butter-Ant Optimization (BAO) approach is applied. The novelty of the suggested approach is that it used a decoded format to transmit the data during encryption and decryption. The encrypted data was then stored in the cloud database for security purposes. The value of Parameter metrics is encryption time (60 ms), throughput (97 Mbps), latency (60 s), execution time (57 ms), security level (98%), and decryption time (55 ms). The

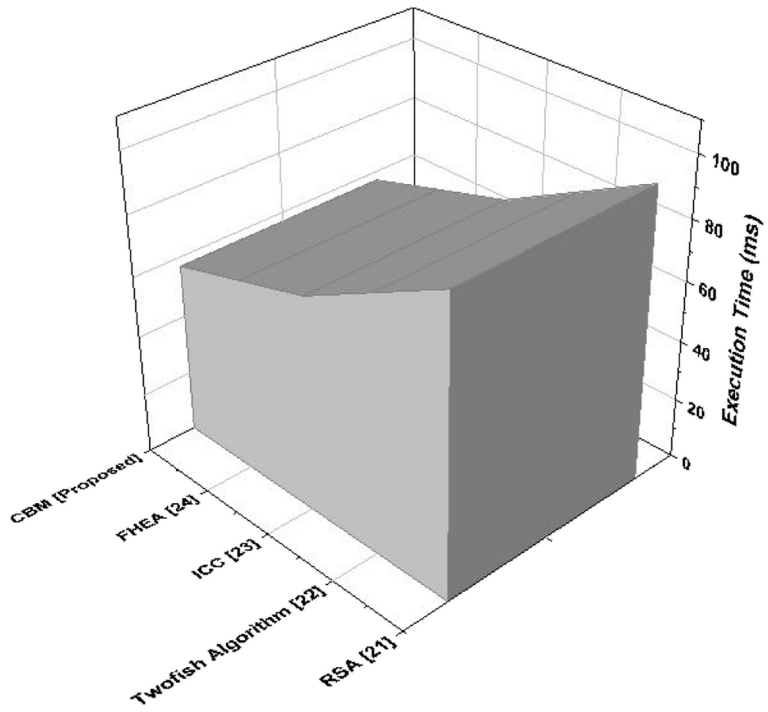


**Fig. 8** Comparative evaluation of execution time

**Table 7** Comparative evaluation of execution time

| Methods | Execution time (ms) |
|---|---|
| RSA [22] | 97 |
| Twofish Algorithm [23] | 84 |
| ICC [24] | 71 |
| FHEA [25] | 64 |
| CBM [Proposed] | 57 |

suggested method is superior to existing approaches for bolstering CPS cloud security [31]. However, energy consumption of the suggested CBM method is not measured for the sensed data which is a shortcoming of this study. The research of different cryptosystems, including hashing algorithms and encryption algorithms [32], may be the focus of future development. It is possible to add more hybrid function layers to further improve the security and integrity of data.

**Acknowledgements**
The authors wish to express their thanks to Vellore Institute of Technology, Chennai, India.

**Authors' contributions**
Author 1 conducted the initial research about the topic and its novelty and designed the model for CPS for carrying out the experiments. Author 2 then created the proposed algorithms Cross Breed and Blowfish and implemented the training dataset and prepared the environment for running the model. The model was built and trained on the input data by Author 3. Author 4 then analyzed the results and recorded them and compared it with other works. Building the environment for adding the modules for further testing of the proposed algorithms and developing the hypothesis was done by Author 5. The author(s) read and approved the final manuscript.

**Funding**
This research is funded by Vellore Institute of Technology, Chennai, India.

**Availability of data and materials**
The supporting data may be provided by corresponding author on request.

## Declarations

**Ethics approval and consent to participate**
There is no ethical approval required and authors express their consent to participate for paper which is a CPS based Cloud Computing and Security in Cloud Computing.

**Consent for publication**
Authors provide the consent for publication which is a health care based on Cloud Computing and Security Computing.

**Competing interests**
The authors declare that they have no competing interests.

**Author details**
[1]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India. [2]Department of Information Technology, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India.

Received: 6 September 2022 Accepted: 21 September 2022
Published online: 12 October 2022

**References**

1. Mbiriki A, Katar C, Badreddine A (2018) December. Improvement of security system level in the cyber-physical systems (CPS) architecture. In: 2018 30th International Conference on Microelectronics (ICM). IEEE, pp 40–43. https://doi.org/10.1109/ICM.2018.8704100
2. Snehi M (2022) Investigating convergence of cyber physical systems and big data analytics to develop real-time defense solution. In: Security and Resilience of Cyber Physical Systems. Chapman and Hall/CRC, pp 37–48. https://doi.org/10.1016/j.engappai.2021.104288
3. Garí Y, Monge DA, Pacini E, Mateos C, Garino CG (2021) Reinforcement learning-based application autoscaling in the cloud: a survey. Eng Appl Artif Intell 102:104288
4. Pivoto DG, de Almeida LF, da Rosa Righi R, Rodrigues JJ, Lugli AB, Alberti AM (2021) Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: a literature review. J Manuf Syst 58:176–192. https://doi.org/10.1016/j.jmsy.2020.11.017
5. Bagula A, Ajayi O, Maluleke H (2021) Cyber physical systems dependability using cps-iot monitoring. Sensors 21(8):2761. https://doi.org/10.3390/s21082761
6. Sailer P, Ivkic I, Tauber M, Mauthe A, Gouglidis A (2021) Analysing design approaches for the power consumption in cyber-physical systems. In: 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE, Bordeaux, pp 908–913
7. Mondal A, Goswami RT (2021) Enhanced honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. Microprocess Microsyst 81:103719. https://doi.org/10.1016/j.micpro.2020.103719
8. Pacheco J, Tunc C, Hariri S (2018) October. Security framework for IoT cloud services. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). IEEE, pp 1–6. https://doi.org/10.1109/AICCSA.2018.8612808
9. Haoxiang W, Smys S (2020) Secure and optimized cloud-based cyber-physical systems with memory-aware scheduling scheme. J Trends Comput Sci Smart Technol 2(03):141–147. https://doi.org/10.36548/jtcsst.2020.3.003
10. Sun Q, Shi Y (2021) Model predictive control as a secure Service for Cyber-Physical Systems: a cloud-edge framework. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2021.3091981
11. Verma J, Bhandari A, Singh G (2022) Recent advancements in the state of cloud security in cyber physical systems. In: Security and Resilience of Cyber Physical Systems. Chapman and Hall/CRC, London, pp 49–60. ISBN 9781032028569
12. Xu Z, Zhang Y, Li H, Yang W, Qi Q (2020) Dynamic resource provisioning for cyber-physical systems in cloud-fog-edge computing. J Cloud Comput 9(1):1–16.1. https://doi.org/10.1186/s13677-020-00181-y
13. Kumar C, Marston S, Sen R (2020) Cyber-physical systems (CPS) security: state of the art and research opportunities for information systems academics. Commun Assoc Inf Syst 47(1):36
14. Trivedi RS, Patel SJ (2022) Security and privacy aspects in the internet of things (IoT) and cyber-physical systems (CPS). In: Handbook of research of internet of things and cyber-physical systems. Apple Academic Press, New Jersey and Canada, pp 453–490
15. Rahman Z, Khalil I, Yi X, Atiquzzaman M (2021) Blockchain-based security framework for a critical industry 4.0 cyber-physical system. IEEE Commun Mag 59(5):128–134. https://doi.org/10.1109/JIOT.2022.3147186
16. Bagheri B, Rezapoor M, Lee J (2020) A unified data security framework for federated prognostics and health management in smart manufacturing. Manuf Lett 24:136–139.1. https://doi.org/10.1016/j.mfglet.2020.04.011
17. Wang Z, Xie W, Wang B, Tao J, Wang E (2021) A survey on recent advanced research of CPS security. Appl Sci 11(9):3751. https://doi.org/10.3390/app11093751
18. Kaur MJ, Riaz S, Mushtaq A (2020) Cyber-physical cloud computing systems and internet of everything. In principles of internet of things (IoT) ecosystem: insight paradigm. Springer, Cham, pp 201–227. https://doi.org/10.1007/978-3-030-33596-0_8
19. Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731. https://doi.org/10.1109/JIOT.2021.3058946
20. Iwendi C, Mahboob K, Khalid Z et al (2021) Classification of COVID-19 individuals using adaptive neuro-fuzzy inference system. Multimedia Systems. https://doi.org/10.1007/s00530-021-00774
21. Iwendi C, Srivastava G, Khan S et al (2020) Cyberbullying detection solutions based on deep learning architectures. Multimedia Systems. https://doi.org/10.1007/s00530-020-00701-5
22. Evsutin O, Melman A, El-Latif A, Ahmed A (2022) Overview of information hiding algorithms for ensuring security in IoT based cyber-physical systems. In: Security and Privacy Preserving for IoT and 5G Networks. Springer, Cham, pp 81–115. https://doi.org/10.1007/978-3-030-85428-7_5
23. Awan KA, Din IU, Almogren A, Kim BS (2022) Fog-Computing-Based Cyber–Physical System for Secure Food Traceability through the Twofish Algorithm. Electronics 11(2):283. https://doi.org/10.3390/electronics11020283
24. Jain DK, Mohan P, Lakshmanna K, Nanda AK (2022) Enhanced data privacy in cyber-physical system using improved Chacha20 algorithm
25. Saad A, Alharbi A (2022) Securing Smart City Services in Cyber-Physical Systems using the computation annealed selection process. Int J Found Comput Sci:1–2. https://doi.org/10.1142/S0129054122420035
26. Iwendi C et al (2021) Pointer-based item-to-item collaborative filtering recommendation system using a machine learning model. Int J Inform Technol DecisMak. https://doi.org/10.1142/S0219622021500619
27. Qadir Md, Abdul; Vijayakumar, Varadarajan, Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering), Volume 13, Number 2, 2020, 260–275(16), Bentham Science Publishers: https://doi.org/10.2174/1872212113666190215145330
28. Iwendi C et al (2021) Security of Things Intrusion Detection System for Smart Healthcare. Electronics 10(12):1375. https://doi.org/10.3390/electronics10121375
29. Md AQ, Vijayakumar V (2019) Dynamic ranking of cloud services for web-based cloud communities: efficient algorithm for rating-based discovery and multi-level ranking of cloud services. Int J Web Based Commun Vol 15(3):248–270. https://doi.org/10.1504/IJWBC.2019.101811
30. Ivkic I, Sailer P, Gouglidis A, Mauthe A, Tauber M (2022) A security cost modelling framework for cyber-physical systems. ACM Trans Internet Technol 2(2):1–31
31. Quadir A, Md V, V., & Mandal, K (2019) Correction to: efficient algorithm for identification and cache based discovery of cloud services. Mobile Netw Appl 24(4):1198. https://doi.org/10.1007/s11036-019-01280-0
32. Md AQ, Varadarajan V, Mandal K (2019) Efficient algorithm for identification and cache based discovery of cloud services. Mobile Netw Appl 24:1181–1197. https://doi.org/10.1007/s11036-019-01256-0

## Publisher's Note