Improving the Security and Authentication of the Cloud with IoT using Hybrid Optimization Based Quantum Hash Function

K. Shankar

Department of Computer Applications, Alagappa University, Karaikudi, India.

Email: shankarcrypto@gmail.com

Abstract

The security with the protection of IoT is to stay a consequential test, for the most part, because of the huge scale and dispersed nature of IoT systems. A cloud server brings wide pertinence of IoT in numerous businesses just as Government parts. Be that as it may, the security concerns, for example, verification and information protection of these gadgets assume a key job in the fruitful coordination of two innovations. To build the security here, a quantum hash work system and hybrid cuckoo search-Artificial Bee Colony algorithm is displayed. A quantum hash work has been presented as an amazing system for secure correspondence of IoT and cloud because of its irregular disordered robust execution, greater affectability for introductory authority dimension, steadiness, and the exceptionally huge crucial area is hypothetically sufficiently able to oppose different known assaults. Cloud servers utilize CS-ABC to upgrade the safe calculations through a quantum channel inside the cloud framework. Execution examinations and recreation outcomes demonstrate our presented methods are portrayed and also have greater safety, and proficiency with strength, as opposed to a few, surely understood assaults which choose them as a great contender for verifying cloud and IoT applications.

Keywords: Cloud; IoT; Quantum hash function; cuckoo search- Artificial Bee Colony; and security.

1. Introduction

The IoT keeps opening up another chance to associate individuals with sensors and gadgets dispersed around their physical world [1]. It has been able to reinforce different applications and organizations in various territories, for instance, quick urban networks and sharp homes. IoT smart items speak with various portions e.g., middle people, PDAs, and data specialists, for the board and data distribution [2]. It is another worldview and an unimaginable innovation for preparing rapidly deployable and versatile data innovation arrangements at traditionalist system transfer speed, decreased framework costs, low idleness, mindfulness, and portability, foundation. It is a proven and dependable response to bring the organizations with resources of the cloud closer to nearer en route for clients [3]. IoT with Cloud Computing benefitted identically and it is continually supported for the Cloud to improve the introduction to the extent of high resource utilization, amassing essentialness, and computational capacity [4]. Cloud is a ground-breaking stage that can give extra accommodations as an information circulation delegate. At the point when an IoT client has legitimate demands for specific information being gathered, put away, and got to, he can straightforwardly designate the solicitations to the cloud whenever with more noteworthy accommodation [5]. The applications of cloud and IoT are made in resource-constrained circumstances with a couple of incites related to contraption disillusionment [6]. To defeat the security issues of IoT a QHF is presented. It maps an old-style message into a Hilbert space so programmers can't get an excessive amount of data about the old-style message [7]. The standard inspiration driving system security information protection is to achieve mystery just as honesty. Safety problems are exceptional essentialness not over-intensifying the dimensions of the system, and devices [8]. D.C calculations have been created for watches out of the said issues; nonetheless, their utilization with the IoT is sketchy when gear client bargain within the IoT isn't fitting for the execution of computationally over-the-top encryption counts [9]. A few calculations are presented in previous papers for safety issues. The U-2 hash work is the biggest class of groups of hash capacities among known classes of groups of hash capacities ensuring solid safety [10].

2. Literature Review

With the quick spread of distributed computing and regularly expanding large information produced by the Internet of Things, remote client confirmation represents the greatest test. Web of Things is a worldview where each gadget in the II-Internet Infrastructure is interconnected into a worldwide dynamic growing system. Sharmaet al. [11] have presented a remote client confirmation conspire for cloud-IoT applications. The plan was lightweight and powerful to assault and has low computational overhead. A proper verification performed utilizing the AVISPA instrument confirms the security of their proposed plan.

To address the basic components and hence understand the cloud-based Internet of Things for an assortment of different application regions, Henzeet al. [12] displayed the UPECSI approach containing an exhaustive arrangement of advancements together with authoritative measures to acknowledge client-driven security implementation for cloud-based administrations in the IoT. They permit an individual client to uphold all her security prerequisites before any delicate information was transferred to the cloud, empower engineers of cloud administrations to coordinate protection usefulness as of now into the advancement procedure of cloud administrations, and offer clients a straightforward and versatile interface for configuring their security necessities.

Yanget al. [13] have shown another hash work by presenting substitute single-qubit coin administrators into DTQW. An exhibited hashing work was traditional and old-style information and yield. The extensive capacity could be executed based on exchange one qubit coin administrators in the state of coin constrained using an old-style incoming twofold information with afterward presented the worldwide restrictive move administrator on coin and position state. Traditional yield hashing esteem was created utilizing enhancement, secluded activity last likelihood conveyance. Mathematical reproduction with execution examination gave the introduced hashing work fantastic applications of crash position with simpler usage over the previous QW-based Hashing. That has advanced more applications quantum calculation of quantum in the plan of hash capacities.

Pleşa and Mihail-Iulian [14] have proposed another plan for secure information transmission dependent on a half-and-half innovation quantum and old style. Their plan tends to two significant issues: the secrecy and uprightness of information. The plan depended on the quantum teleportation circuit yet the information transmission was cultivated through traditional stations. A few tests were directed utilizing the new IBM Q stage.

Chenget al. [15] have presented quantum-safe crypto frameworks for verifying security in IoT. They initially exhibited an effect Q-PCs for current security of crypt-systems afterward gave a proposal reviews for crypt-systems plans could be safe in the assaults of Q with traditional PCs. They were first shown the impacts of quantum PCs on the security of the cryptographic plans used today, and a short time later give an audit of the proposition for cryptographic plans that could be secure under the ambushes of both conventional and quantum PCs. From that point onward, they exhibited the current usage of quantum-safe cryptographic plans on compelled gadgets appropriate for the Internet of Things. At long last, they gave a prologue to progressing ventures for quantum-safe plans that would assist with building up the future security answers for the IoT.

3. Problem Formulation

- To approve the client's acknowledgment of complete methodology UPECSI's further specialized development will firmly be attached to criticism circles of a participatory plan approach [16]. Thusly, effectively fuse different intrigue gatherings (e.g., end-clients, administration designers, and specialists) into the further improvement process. This engages partners as dynamic individuals for the future advancement of UPECSI and henceforth causes us to expand client acknowledgment. This is one of the major testing issues in IoT [17].
- To diminish the extra exertion required for improving cloud administrations with protection capacities, we need to offer help for designing security into the administration and facilitate the survey of this usefulness [18].
- Security moves toward that rely extraordinarily upon no encoding is a strong counterpart that obliged contraptions none of them were prepared for processing a complicated encoding with decoding quickly to transfer data securely in a dynamic way. A Major safety problem in IoT is labeled assault [19].
- The information entrance must be verified and must be controllable by the proprietor of this information. Be that as it may, the security systems must be flexible enough to represent unconstrained personality changes about protection when clients are in physical peril [20-22].

4. Methodology for IoT and Cloud Security

Right, when the IoT splendid contraptions share data with various devices, potential safety problems arise, for instance, data emission, conversion, integrity, and unapproved find a good pace. Hence, such common data must be ensured safety, decency, and access control while sharing at the edge. Additionally, an ensured data sharing system is required to share and recoup the regular data by affirmed contraptions. Here, we presented two techniques to examine the challenges of data safety participating in fogs. From the outset, we revolve around the DTQW model which is used to create QH and can able to design the presented safety instruments of IoT applications. Based on the coin directions the QW are compelled in the DTQW. Typically, the amount of QW and QC is extraordinary. The quantum Hash work in the message confirmation plan ought to be effectively executed in comparing programming.

The information validation plot, QH esteem is created by applying one QC and QW. In this way, our quantum Hash work has no challenges in programming usage. Also, we introduced half-breed CS-ABC used to encode and share information put away in cloud servers. IoT gadgets can store and share their information by using the half-breed CS-ABC to encode the information before putting away it in the distributed storage. The proposed procedures have a few focal points, for example, barriers against different sorts of assaults and safety ensured by Q-behaviours. Subtleties of ideal CS-ABC with hash work are clarified in the underneath area.

4.1 *Analysis of security and privacy in IoT applications*

Security in IoT is troublesome on account of the low resource capacities of most by far gadgets, immense scale, heterogeneity among the devices, and nonattendance of institutionalization. Furthermore, an impressive many of these devices' contraptions assemble provided a lot of data sources relative to individual places, thusly presenting a vital security concept. Safety with protection chance investigation of an ordinary clever home building that relies upon OFF immediately in the mart of devices with the steps. Instead of OFF safety with danger examination of this device transfer to circumstances, we center on a real IoT brilliant home behaviors sent in our tried focusing an association in the various device parts.

4.2 *Generation of IoT data*

It has certain characteristics; that introduce broad dimension information that needed a system force towards critical timeframes.

Pre-processing

This fundamental pre-preparing information is isolated to pick the touchy aspects of safety data for, the reason pre-handlings are decreasing the processing period. Also, the objective is to guarantee fruitful safety and enhance the exhibition of the model, we secure delicate information as it were. IoT information grouping utilizing streamlining Information is bunched by using a sporadic grouping model with enhancement. Every datum is surveyed by loads of its bunch affiliations. At last, among different hubs and as demonstrated by their loads a hub is chosen as the bunch head, for ideal group head determination CS-ABC improvement is proposed. At long last, among different hubs and as appeared by their data a hub is chosen as the bunch head.

4.3 *Hybrid CS-ABC Algorithm*

Bees of the ABC model plan to find the best course of action. While the circumstance of a sustenance source shows a potential response for the progression issue, the nectar proportion of a sustenance source analyses the quality (wellbeing) of the related game plan. This half-and-half calculation is used in the choice of bunch heads for the protection and safety model.

All of the used bees share their information with the spectators and with afterward, visit the sustenance source locale visited by her in the past rolling's using the data staying in her memory about the past sustenance source. At the point when the past sustenance source is gone too, the used bumblebee picks another sustenance source through visual data in the zone of the one in her memory and evaluates the measure of nectar in the new sustenance source. The area of phony bees involves three social affairs of bees,

a. Employee bees,
b. Onlookers
c. Scouts.

a. Employee Bee

A bee that outstanding parts in the move locale to pick which sustenance source is to be picked viewed as an observer and a bee that lands at the sustenance source visited by it as of now are named a used bee. A bee that performs subjective requests is known as a scout. The first half of the state is included by the used fake bumblebees and the ensuing half is included by the onlookers. Each sustenance source has only one used bumblebee. This proposes the used bees and the sustenance sources around the hive are number insightful equivalent.

In the hidden stage, used bumblebees pick a great deal of sustenance source positions emotionally and choose their nectar aggregates. By then, they return to their hive and prompt about the nectar signifies the spectator bumblebees, which are holding up in the moving section of the hive. ABC from the start makes a discretionarily passed on beginning people, which has n game plans, where each course of action addresses a sustenance source position and addresses masses size. Each course of action can be addressed where V-vector segments are the number of headway parameters pondered. At the point when the reinstatement process is done, the quantity of occupants in positions is presented to iterative glancing through methodology engaged by used bumblebees, onlooker bees, and scout bees.

b. Onlooker Bee

This stage enables passerby bees to pick the sustenance sources reliant on the information given by the used bees followed by delivering new courses of action. The spectator bumble bee depends upon the nectar information appropriated by the used bees on offering a tendency to the sustenance source. The probability of picking a sustenance source by a passerby bee increases, when the nectar proportion of the sustenance source increases. Subsequently, spectator bees are chosen for the used bumblebees that have higher nectar because of the richness of the sustenance source. The probability plan P_f for a passer-by bumblebee to pick a sustenance source is given beneath,

$$\phi = \frac{f_{sol}}{\sum_{q=1}^{N} f_q} \tag{1}$$

f_{sol} - Fitness arrangement, f_q - q source wellness esteem, N-No. of. nourishment source = No. of utilized honey bees.

The spectator bee lands at the picked sustenance source and finds sustenance sourced from the neighborhood locale subject to the memory of visual information. Visual information is made dependent on the assessment of sustenance source positions. By neglects of any sustenance source as a result of its low nectar total, the scout bumble bee is consigned to displace the abandoned sustenance position with another optional sustenance source position. The phony spectator bee performs probabilistic enhancements for the position (course of action) in the memory to find a new sustenance source and surveys the nectar whole (health estimation) of the new source (new game plan).

The existing situation $O^{p}{}_{i,x}$ and current situation $N.^{p}{}_{i,x}$ and the separate illustration are given below,

$$O^{p}{}_{x} = N^{p}{}_{x} + \psi^{p}{}_{x}(N^{p}{}_{x} - N^{q}{}_{x}) \ \ , \ p \neq q \tag{2}$$

Where, x, q= [1,2,…..,N], $\psi^{p}{}_{x}$ - arbitrary integer from -1 to 1.

The condition of an updated situation is generally understood that a decrease in deflection $N^{p}{}_{x} \ \ to \ \ N^{q}{}_{x}$. Thusly, an amazing diminishing of step length is enabled here, when the perfect course of action from the interest space is moved closer by the chase procedure. The spot reviving development can be adjusted as given underneath,

$$G_{t+1} - G_t = \psi_{p,x}(N^{p}{}_{x} - N^{q}{}_{x}) \tag{3}$$

Time domain - $O^{p}{}_{x}$ this is the updating place from $N^{p}{}_{x}$

Where,($G_{t+1} - G_t)$ - discrete version ψ =1

$$Q^{\beta}[G_{t+1}] + \Psi^{p}{}_{x}(N^{p}{}_{x} - N^{q}{}_{x}) \tag{4}$$

Here, rather than the scout honey bee, we utilize cuckoo search calculation for better optimization.

4.4 *CS- Algorithm*

The Cuckoo search algorithm speaks to a mimetic calculation that owes its birthplace to the rearing behavior of the cuckoos and it is simple in execution. There are a huge number of homes in the cuckoo search. Each egg connotes an answer and an egg of a cuckoo compares to a novel arrangement. The epic and unrivaled arrangement replaces the most awful arrangement in the home. The business as usual of the bunching system is appeared as below:

i. Initialization

The populace Sp, p= 1,2,… …, N of the host home is self-assertively started. At that point, it creates a new cuckoo stage has appeared in condition 5,

$$O^{p}{}_{x} - N^{p}{}_{x} = \psi^{p}{}_{x}(N^{p}{}_{x} - N^{q}{}_{x}) \tag{5}$$

With the assistance of the levy flights, a cuckoo is chosen haphazardly which creates novel arrangements. Therefore, the incited cuckoo is assessed by utilizing the target work for determining the greatness of the arrangements.

ii. *Calculation of fitness*

The wellness work is assessed as per Equations 6 and 7 demonstrated hereunder, trailed by the choice of the good one.

$$pop_{\max} = \frac{sel_{pop}}{tot_{pop}} \tag{6}$$

$$f = pop_{\max} \tag{7}$$

Where, sel_{pop} - selected population, tot_{pop} -total population

iii. Update function

At the start, the arrangement is optimized by the levy flights by utilizing the cosine change. The nature of the novel arrangement is assessed and the home is chosen discretionarily from among them. If the nature of the novel arrangement in the chosen home is better than the past arrangement, it is supplanted by the novel arrangement (Cuckoo). Something else, the past arrangement is treated as the best arrangement. The levy flights utilized for the general cuckoo search calculation are communicated by Equation 8 demonstrated as follows:

$$h_p^* = h_p^{(N.P+1)} = h_p^{N.P} + \beta \oplus L(N) \tag{8}$$

By appropriately adjusting Equation 8, the demand flight condition utilizing the gauss conveyance is displayed in condition 9 hereunder:

$$h_p^* = h_p^{(N.P+1)} = h_p^{N.P} + \beta \oplus \lambda(O.P) \tag{9}$$

$$\lambda(O.P) = \lambda_0 \exp(-\gamma_g) \tag{10}$$

Where, λ_0, γ = Constants

iv. Exclude the poorest nest

In this area, the most noticeably awful homes are disregarded, as per their plausibility esteems and novel ones are built. Consequently, contingent on their wellness work the best arrangements are positioned. From that point, the best arrangements are identified and set apart as ideal arrangements.

v. Termination

Till the accomplishment of the most extreme emphasis, the methodology is preceded.

4.5 *Quantum Hash Mechanism for IoT*

This research content is an idea related to the QW work that is QW. All in all, QW is for the most part isolated as ceaseless time QW and DTQW. We append significance to the DTQW.

i. DTQW

In the DTQW, walkers are obliged by coin executives. Typically, at present, the amount of walkers and coins is variable. There are a couple of positions, which are coin position and walkers position then the whole space is H(Hilbert)P is given underneath,

$$K = K^{\varphi} \otimes K^{\omega} \tag{11}$$

Where, K-Hilbert space, K^{φ} - Coin space, and K^{ω} - Walkers space

The development of the walker is constrained by the restrictive move administrator η as given below,

$$\eta = \sum (|z+1\rangle\langle z| \otimes |0\rangle\langle 0| + |z-1\rangle\langle z| \otimes |1\rangle\langle 1|) \tag{12}$$

This shows the summation over every conceivable position. The entire procedure is heavily influenced by the coin-flipping administrator and the restrictive move administrator. The coin flipping administrator is demonstrated as follows,

$$F \otimes \varphi \tag{13}$$

Where F is the personality administrator who holds the walker and φ is the coin rolling director presented in the direction of the coin. In the circle position, use the character director F, the walker in the direction clockwise. Along with this, the Pauli chairman is used on the hover, and by then, the walker on opposite to clockwise. The walker's directions appear in Fig. 1, the one-coin one-walker quantum walk occurs on the circle, the center number of which is N.

$\varphi\ \sigma_x$

Figure 1: The potential bearings W-strolls on the circle. (a) Heavily influenced by coin administrator φ . (b) Bearing is anticlockwise heavily influenced by the coin administrator σ_z .

4.6 *Quantum Hash Function*

Single direction Hash capacity is depicted in a detailed manner. Picking the verification work, all consider single direction QW work. The principal characteristics of H-work are the single path, solid impact opposition, and frail crash obstruction. The properties of the quantum Hash capacities are given as follows,

Single-direction

Given a data D, it is possible to process the H regard H(D) while it is infeasible to locate the fundamental data D with a given H regard H(D)computationally.

Frail crash obstruction

Given a data D, it is infeasible to find another data D1 computationally so that H(D)=H(D1).

Solid impact opposition

It is infeasible to find optional two unmistakable data D and D1 computationally so that H(D)=H(D1).

These three properties are central models worth pondering when grasping an H work.

Contrasted and old-style Hash work, quantum Hash work has more favorable circumstances, for example, simple execution, and a more significant level of security. our information confirmation plan will be progressively secure. The nitty-gritty procedure of the quantum Hash work is portrayed as shown below,

Select the parameters [m, $\theta 1$, $\theta 2$, τ] under the requirements: m is an odd number and $\{0 < \theta 1, \theta 2, \tau < \frac{\pi}{2}\}$ Here τ - coin state $|0\rangle = \cos\tau|0\rangle + \sin\tau|1\rangle$, m- No. of cycles. In addition, $\theta 1$ and $\theta 2$ - controller of two C-QW.The admin of two coin controllers is φ^1 and φ^2 .

$$\varphi^1 = \begin{bmatrix} \cos\theta 1 & \sin\theta 1 \\ \sin\theta 1 & -\cos\theta 1 \end{bmatrix}, \quad \varphi^2 = \begin{bmatrix} \cos\theta 2 & \sin\theta 2 \\ \sin\theta 2 & -\cos\theta 2 \end{bmatrix} \tag{14}$$

The underlying one- information bit chooses φ^1 with "0" chooses φ^2 . Rolling the one coin and walker DTQW on a cycle is heavily influenced by information D and creates the likelihood of dispersion. Intensify all qualities in the subsequent likelihood circulation by 10i occasions and keep just their whole number part modulo 2jto frame a twofold H calculation, $i \geq j$. The bit length of the H regard is mj. This is the methodology of the latest QH works conspire, whose safety is higher than past ones. Deservedly, we decide to get this QH ability to be the approval work.

4.7 *Encryption*

Encryption framework functions as given data and a key; it makes a figured data to be transferred over un-safe channels, with no peril being comprehended by other people who don't have the interpreting key. For safety reasons, the key is subject to a couple of sets, initially, open and one private key. At first, to encode, second to disentangle and the different way; conceivable because of the use of some mathematical limits have the characteristics of non-reversible.

Scrambled, unscrambled data,

$$Encryption = H(amount\,of\ I/P, H, openkey, I/P) \tag{15}$$

$$Decrypt \Rightarrow ((m^k)\,|\,\mathrm{mod}\,ified\ \ I/P(E)\,|)*open\,key \tag{16}$$

Hash works capably transmits on limited info to yield string with the permanent H knew length esteem. In light of this worth, the IoT sight and sound data are verified by the quantum value, open keys and confined irregularity has able to abuse bargain the H-esteem. Accommodating components yet ought to be described to ensure the security of exchanges simultaneously stay away from race assault.

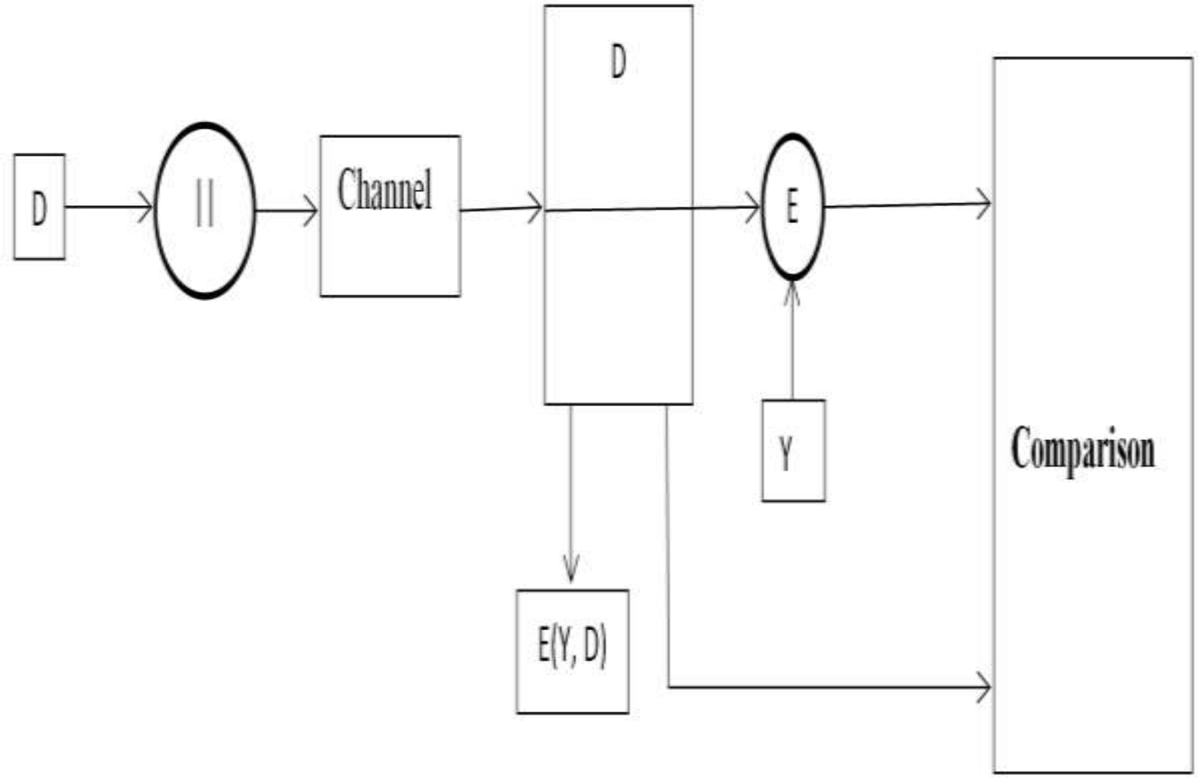

Figure 2: Architecture of data authentication using hashing mechanism.

Fig.2 shows the general procedure of information confirmation. D is the underlying information that will be moved from the sender to the recipient. E is the verification work used to scramble the underlying information D. "‖" is an activity used to course the underlying information and the figure writings. The square edge is utilized to represent the channel during correspondence. Y is the key used to encode the underlying information.

5. Result and Discussion

The presented IoT information safety model is processed in the working platform of Java included with the JDK 1.7.0 in windows ME, for instance, the Intel (R) Core i3 processor, 1.6 GHz, 4 GB RAM, and we use Microsoft Window7 Professional.

Table 1 shows the delayed consequence of the presented grouping model. Here we select the number of gatherings subject to the size of the information base. It takes the size of the information base depending on kilobytes, for example,

We pick 10 kb to 50 kb. Our presented technique accomplishes group one obtains 5, bunch two achieves 2, group 3 as 1, and bunch 4 as 0. So also, different databases accomplish the best determination in the CS-ABC model. The above-said assessments are envisioned in figure 3.

Table 1: Analysis of proposed clusters number

Database size (kb)	No. of clusters (kb)			
	Clus.t1	Clust.2	Clust.3	Clust.4
10	4	1	3	2
20	8	6	0	7
30	9	16	6	4

40	18	7	8	10
50	11	14	19	13

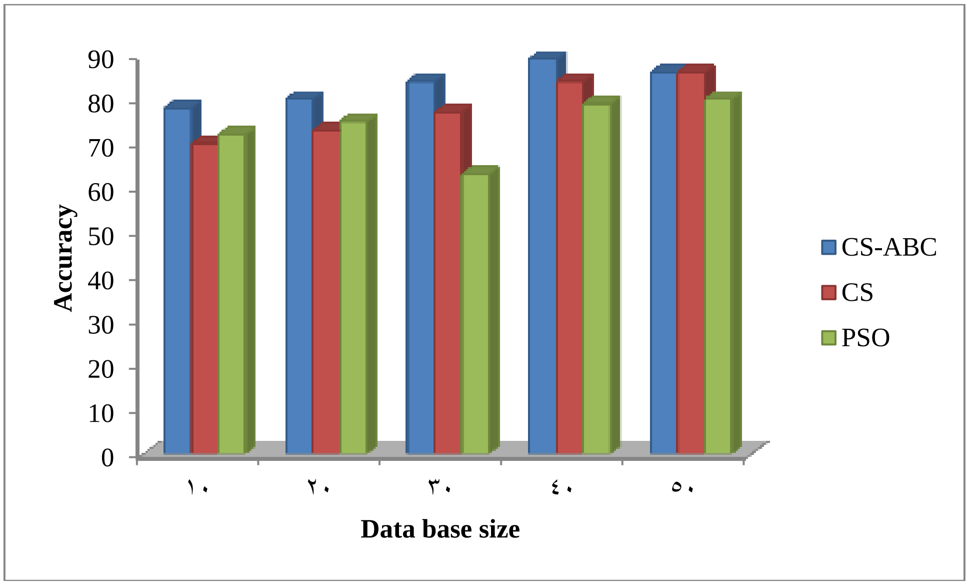

Figure 3: Accuracy of cluster

Table 2: Results of quantum hash mechanism

Size of the files	Encryption	Decryption	Memory (byte)	Processing period (ms)
10	28	10	2165636	87321
20	37	20	467897	942749
30	48	30	476756	10987
40	51	40	576654	113456
50	59	50	563422	115675

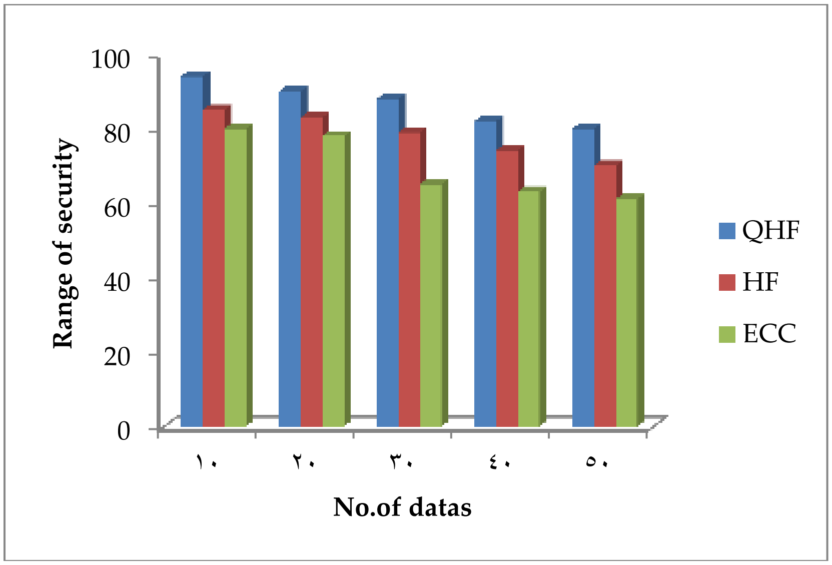

Figure 4: No. of data with the quantum hash value

Table 2 and figure 4 show the eventual outcome of the presented parameters which get in the assessment. Depending upon record size, we find encryption size, disentangling size, memory, and execution time. The result depicts that encryption size and unscrambling augmentations if the archive size extended, the execution time furthermore extended. In any case, diverged from various methodologies presented model secures the IoT data in a high manner.

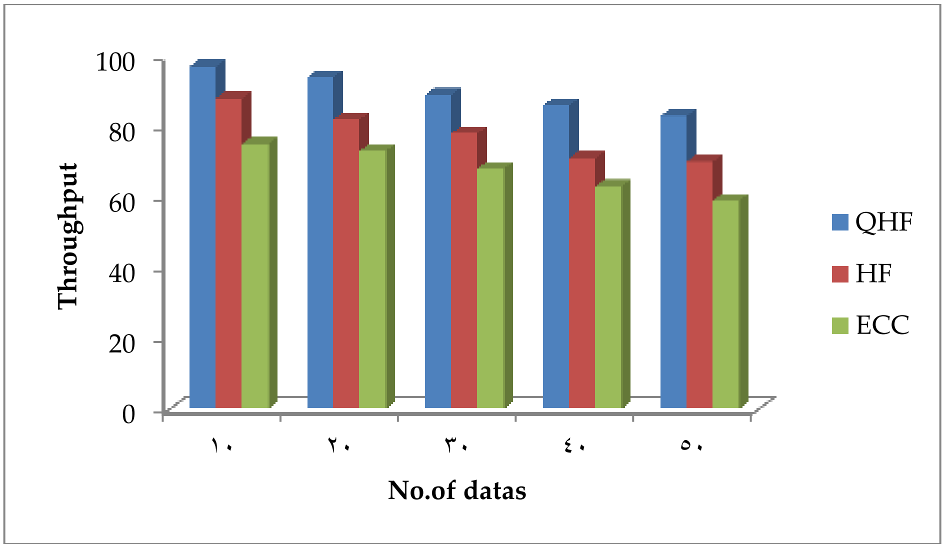

Figure 5: No. of data with throughput value

Figure 5 shows the throughput level reliant on the database size. The QH work plays out a perfect safety level for every information base size. The level throughput lands at a generally outrageous 90% in QH work.

6. Conclusion

Distributed computing and IoT have prompted the progression of various applications that grant clients to get to information anyplace whenever. This paper displayed a quantum hash work component and half-breed cuckoo search-Artificial Bee Colony calculation. A quantum hash work has been presented as a phenomenal instrument for secure correspondence of IoT because of its nonlinear disorganized dynamical execution and huge keyspace hypothetically sufficiently able to oppose different known assaults. Cloud servers utilize CS-ABC to upgrade the protected calculations through a quantum channel inside the cloud foundation. The benefits of quantum hash work, in this research work, presented the latest developments for accomplishing a safety data distribution and information insurance that is depending on Q-advances. Directed execution investigations and reproduction results demonstrated the presented methods are described beside greater precision, safety, throughput, and heartiness over a few surely understood assaults which make them reasonable for usage inside different IoT and cloud applications.

References

[1] Wang, King-Hang, Chien-Ming Chen, Weicheng Fang, and Tsu-Yang Wu, "A secure authentication scheme for Internet of Things," Pervasive and Mobile Computing, Vol. 42, pp. 15-26, 2017.

[2] Geneiatakis, Dimitris, IoannisKounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and GianmarcoBaldini, "Security and privacy issues for an IoT based smart home," In process of 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1292-1297, 2017.

[3] El-Latif, Ahmed A. Abd, BassemAbd-El-Atty, M. Shamim Hossain, Samir Elmougy, and Ahmed Ghoneim, "Secure quantum steganography protocol for fog cloud Internet of Things," IEEE Access, Vol. 6, pp. 10332-10340, 2018.

[4] Yang, Zhe, Qihao Zhou, Lei Lei, KanZheng, and Wei Xiang, "An IoT-cloud based wearable ECG monitoring system for smart healthcare," Journal of medical systems, Vol. 40, No. 12, pp. 286, 2016.

[5] Wang, Wei, PengXu, and Laurence T. Yang., "Secure data collection, storage and access in cloud-assisted IoT.," IEEE cloud computing, Vol. 5, No. 4, pp. 77-88, 2018.

[6] Stergiou, Christos, Kostas E. Psannis, Brij B. Gupta, and Yutaka Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT." Sustainable Computing: Informatics and Systems, Vol.19, pp. 174-184, 2018.

[7] Yang, YuGuang, YuChen Zhang, Gang Xu, XiuBo Chen, Yi-Hua Zhou, and Weimin Shi, "Improving the efficiency of quantum Hash function by dense coding of coin operators in the discrete-time quantum walk," SCIENCE CHINA Physics, Mechanics & Astronomy, Vol. 61, No. 3, pp. 030312, 2018.

[8] Srinidhi, N.N., Kumar, S.D. and Venugopal, K.R., 2018. Network optimizations in the Internet of Things: A review. Engineering Science and Technology, an International Journal.

[9] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems.

[10] Tsurumaru, Toyohiro, and Masahito Hayashi. "Dual universality of hash functions and its applications to quantum cryptography." IEEE transactions on information theory, Vol.59, No. 7, pp. 4700-4717, 2013.

[11] Sharma, Geeta, and SheetalKalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," Journal of information security and applications, Vol. 42, pp. 95-106, 2018.

[12] Henze, Martin, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, Bernhard Rumpe, and Klaus Wehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," Future Generation Computer Systems, Vol. 56, pp. 701-718, 2016.

[13] Yang, Yu-Guang, Jing-Lin Bi, Xiu-Bo Chen, Zheng Yuan, Yi-Hua Zhou, and Wei-Min Shi, "Simple hash function using discrete-time quantum walks," Quantum Information Processing, Vol. 17, No. 8, pp. 189, 2018.

[14] Pleşa, Mihail-Iulian, "Hybrid scheme for secure communications using quantum and classical mechanisms," In process of 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1-6, 2017.

[15] Cheng, Chi, Rongxing Lu, Albrecht Petzoldt, and Tsuyoshi Takagi, "Securing the Internet of Things in a quantum world," IEEE Communications Magazine, Vol. 55, No. 2, pp. 116-120, 2017.