Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1427–1436
DOI : 10.47974/JDMSC-1768

Machine Learning (ML)–centric resource security in cloud computing using authenticated key

Ravi Shankar Saxena [$]
Department of Electronics & Communication Engg.
GMRIT
Rajam
Vizianagram
India

Smaranika Mohapatra [†]
Department of Information Technology
Manipal University Jaipur
Jaipur
Rajasthan
India

Amit Kumar Singh [§]
Amity Institute of Information Technology
Amity University Rajasthan
Jaipur 302001
Rajasthan
India

Bhupati [‡]
Department of IoT
K. L. Deemed to be University
Vaddeswaram
Guntur 522302
Andhra Pradesh
India

[$] *E-mail:* ravishankar.s@gmrit.edu.in
[†] *E-mail:* smaranika.mohapatra@jaipur.manipal.edu
[§] *E-mail:* aksingh1@jpr.amity.edu
[‡] *E-mail:* bhupati@kluniversity.in

Juan Carlos Cotrina-Aliaga [@]
Faculty of Human Medicine
Universidad Privada San Juan Bautista
Chincha
Perú

José Luis Arias-Gonzáles [#]
Pontificia Universidad Católica del Perú
Perú

Sarvesh Kumar*
Department of Computer Science & Engineering
Babu Banarasi Das University
Lucknow
Uttar Pradesh 226028
India

Abstract

The computing is the on-request transportation of registering contributions over the web to give speedier advancement, bendy assets, and economies of scale. Administrations incorporate servers, stockpiling, data sets, systems administration, programming, and examination. The routine security tasks that the providers carry out include protecting the basic system, reaching, maintaining, and setting up the actual has and organization, on which the strategy illustrations run, as well as the capacity and unique possessions.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Cloud parameters, Security issues, Machine learning, Security parameters, Cloud services, Cloud security simulation.*

1. Introduction

Cloud computing manages the cost of an organization's speed, efficiency, charge reserve funds, execution, and security. Cloud-based capacity makes it feasible to keep records in a distant and recover them on request. Cloud computing probably offers hugely restorative transporter to the client, nonetheless, still, many organizations do now not guide cloud computing contributions because of the reality of assurance imperatives

[@] *E-mail:* **juan.cotrina@upsjb.edu.pe**
[#] *E-mail:* **a20225538@pucp.edu.pe**
* *E-mail:* **Kr.sarvi91@gmail.com (Corresponding Author)**

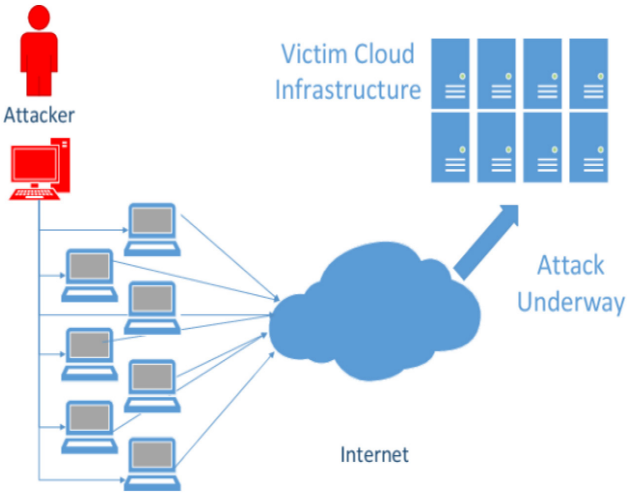

Figure 1

Basic attacks in cloud services

[1]. The principal insurance punishments are insights wellbeing and privateness security. This security dilemma prevents the administrators, clients, or customers from building up the contributions provided by means of cloud computing innovations [2][3]. Figure 1 explains the cloud service attacks going now adays. There should be a reliable and confident relationship of certainty among clients and chiefs sooner than profiting of any cloud administration. The trustworthy gathering ought to have the authorized organization group's commitment to guarding the security risks of impenetrable cloud information[5][6].

While sending data it is typically indispensable to hide from looking contraptions on the web. Information is a valuable guide to any business and individual, and the charge of moving realities to the cloud is developing every single day. The biggest task in arriving at distributed computing wellbeing is to resistant information, this is because of the reality customers depend on the supplier merchants to ensure that the records is secure [7]. The homes of records assurance kept up with through the cloud incorporate secrecy, trustworthiness, approval, data accessibility, and security. Ill-advised managing of measurements with the guide of the cloud may moreover prompt records dangers, which comprise of data break, realities misfortune, honesty infringement, and unapproved access [9].

2. Related Work

The research is moving in a vast way in the computing system which was once assessed that come 2020 there will be an extraordinary many amazing gadgets and gadgets, which is nowadays completely evident [8]. The dispensed figuring advancement separates and shops insights capably, this enrolling development has servers that are converged on cloud stages, for instance, cloud service providers to engage sharing of resources, which can be gotten to at any spot and time using the web[10]. Figure 2 explains the different risks in the cloud to the end users and the service provided by the CSPs.

Cloud computing is a significant piece of IoT that consolidates the servers, separates records got from the sensors, increases overseeing power, and offers great possible cutoff points. Cloud computing is facilitated with astute articles which utilize a few sensors and helps IoT for a huge degree improvement. IoT relies on apportioned processing and each figuring advance countenances insurance risks. Since the 1960s, cloud computing thoughts have been introduced by using experts and PC researchers. Because of a few get away clauses and much less registering electricity in the cloud framework, a few significant anticipated purchasers and associations are no longer adjusting to the cloud approach. To overcome this obstacle, in 2006, Amazon dispatched off its cloud stage named AWS (Amazon Web Services), from which the cloud transformation began. This assisted with addressing provisos that blanketed examination of method

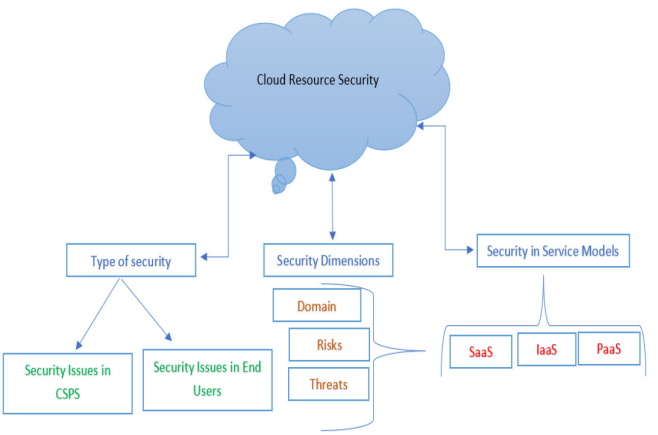

Figure 2

Cloud security system

and engineering of specific cloud stages, their correlation, and digital safety perspectives.

Security is one of the primary assignment cloud functions faces today. Subsequently, brilliant many humans are reluctant to go to cloud-based arrangements. In 2008 an overview was once directed by way of International Data Cooperation (IDC) utilizing 244 IT leaders and CIO and 74.6% of them identified protection as the crucial check in allotted computing. At the factor when you reflect on consideration on verification security, we should see a few safety breaks passed off at some stage in the past couple of years. As per the wholesale fraud asset focus, there have been 498 all out protection breaks had been accounted for in 2009 [15]. In any case, internal the preliminary 4 months of 2010 there have been 245 safety breaks had been accounted for, and the widespread majority of these protection breaks occurred due to the fact of taken passwords or hacking passwords. Accordingly, affirmation safety capability pretty a bit to any type of utilization[17]. In cloud verification, quite a number methodologies are been utilized. As per the cloud sending mannequin verification techniques receives particularly special for occasion affirmation implies utilized in exclusive cloud is particularly now not pretty the identical as validation suggest utilized in extensive sunlight hours mists [18].

3. Research Challenges in cloud Security

A portion of the high-level cloud-local security challenges and the numerous layers of hazard looked by the present cloud-situated associations include:

First are the attackers attacking on the cloud environment. The public cloud local weather has grown to become into a big and rather attractive assault floor for programmers who take advantage of inadequately received cloud entrance ports to get to and upset obligations and facts in the cloud [4]. The second major issues of the cloud security are the risk in IaaS system in cloud. The primary layer is completely under the control of the cloud providers in the IaaS marketplace, and they conceal it from their customers. The PaaS and SaaS cloud models show a need of reasonableness and permeability [8]. Cloud customers frequently lack the ability to truly photograph or measure their cloud natural components. The third major type of attack is the key management security of cloud services. Frequently cloud customer jobs are designed freely, permitting vast honors previous what is anticipated or required [13]. Figure 3 defines the major ways of cloud securities in cloud service.

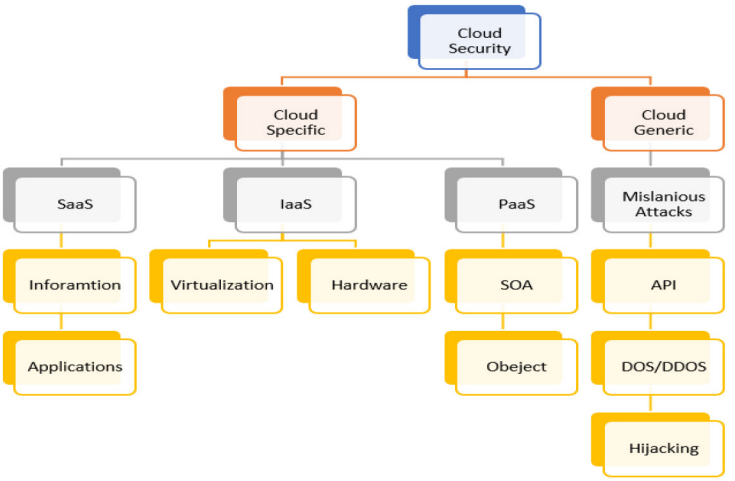

Figure 3

Types of cloud computing security.

4. Proposed Methodical Structure

We propose an identity based key exchange scheme which avoids pairing in any steps. Our algorithm provides address the key escrow problem, known key secrecy, perfect forward secrecy, key compromise impersonation, and security against key control.

In this research we have proposed the algorithm as shown below.

Proposed Algorithm: This proposed algorithm is forming the secure nature of the cloud services to identify key exchange.

Input: The cloud resources in which security is applied. In setup phase KGC selects the system parameter and generate the secret key s.

Output: Different cloud service providers form the optimal allocation of the cloud services.

1: **Begin:**
2: **For** Security system in service apply:
3: **Step1**:
4: *Selects a large n bit prime number p.*
let E be the elliptic curve defined over Fp.
5: **For Each** Service the encryption:
Step2:
6: *Selects a arbitrary random point*
$P \in E/Fp$ *of order q.*

7: **For Each** Modify the key value of the iteration every time.
8: **Step3:**
9: $Selects\ a\ random\ s\ \in Zq.$
10: **STEP 4**
11: $Computes\ the\ master\ public\ key\ PKGC\ =\ s{:}P_{.1}$
12: **STEP 5**
13: $Chooses\ a\ hash\ function\ H1:\ 0;\ 1 \rightarrow\ E.$
14: **STEP 6**
15: $Publishes\ (P;\ PKGC)\ for\ public\ uses.$
End.

4.1 *Experiments and results:*

We analyze our algorithm and show that it is secure against key escrow problem, key control, key compromise impersonation and achieve forward secrecy. Figure 4 explains the key generation system in cloud security. This algorithm can be efficiently implemented in devices with low computational capacity and limited battery power such as PDAs and mobile phones. The table 1 explains the bit size required for different types of cloud services.

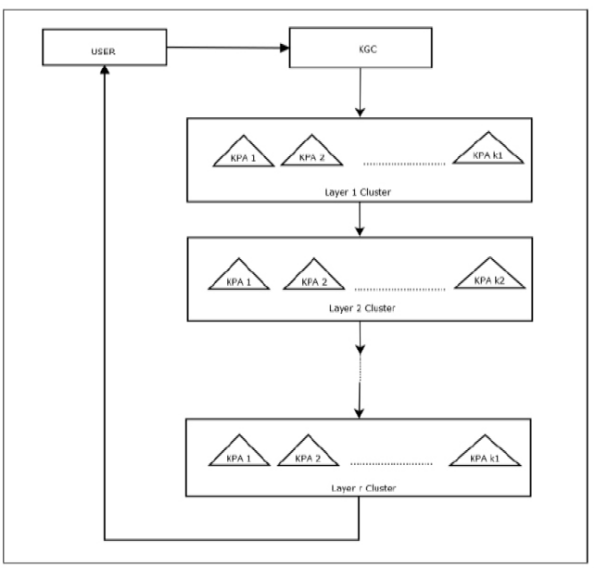

Figure 4

User Key generation system

Table 1

NIST defined bit length of the key

Bit Length of n	Prime Field
161 ---- 223	Lens(P)=192
224 ---- 255	Lens(P)=224
256 ---- 383	Lens(P)=256
384 ---- 511	Lens(P)=384
=>512	Lens(P)=521

The calculated direction, which is based on two organized accentuations prepared, is the foundation of the proposed methodology. The outcome of the subsequent step is input for the taking after arrangement in a special calculated outline. In any case, in a balanced important direction, some parts of the previous step and the current step determine the commitment for the arrangement that follows. The key estimate in the proposed method is 128 digits, which is sufficient against a brutal control ambush. Every eight rounds, the subkeys are changed (Table 2). As a result, locating the aggressor's primary key at any time is challenging. When calculating that the qualities are denser for an input picture than appropriated for an encoded picture, the scattering of the pixel values ought to be obvious.

Table 2

Comparison of correlation coefficient

	Image File taken as Input	Cipher Image		
		Cipher Image in	The encrypted image of file	Proposed method
H- index	0.832	0.0043	0.023	0.004
V- index	0.821	0.00021	0.013	0.00053
D system	0.819	0.00012	0.0015	0.00064

5. Conclusion and Future Work

Cloud computing is normally utilized and embraced all through the world subsequently IoT depends on the cloud considering the limit of records and assets. The two taking care of upgrades face protection risks and it is a colossal issue. It is quintessential to lessen protection

bothers to set aside with the certainty and respectability of clients. IoT and Cloud figuring enhancements are progressing rapidly consequently clear security is required.

References

[1] Kumar, S., Srivastava, P. K., Srivastava, Singh, D., & Goyal, D. Chaos based image encryption security in cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1041-1051 (2022).

[2] Kamble, S., Saini, D. K. J., Verma, S., Tiwari, A., & Goyal, D. Detection and tracking of moving cloud services from video using saliency map model. *Journal of Discrete Mathematical Sciences and Cryptography,* 25(4), 1083-1092 (2022).

[3] Kumar, S., Dubey, K. K., Gautam, Kumar, V., & Mamodiya, U. Detection of recurring vulnerabilities in computing services. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 1063-1071 (2022).

[4] Kumar, S., Kumar, S., Ranjan, N., Tiwari & Rafsanjani, M. K. Digital watermarking-based cryptosystem for cloud resource provisioning. *International Journal of Cloud Applications and Computing* (IJCAC), 12(1), 1-20 (2022).

[5] Tiwari, Ashish, and Ritu Garg. "Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems." *International Journal on Semantic Web and Information Systems* (IJSWIS) 18, No. 1, 1-18 (2022).

[6] Rangaiah, Y. V., Sharma, A. K., Bhargavi, T., Chopra, M., Mahapatra, C., & Tiwari, A. (2022, December). A Taxonomy towards Blockchain based Multimedia content Security. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1-4. IEEE.

[7] Rohinidevi, V. V., Srivastava, P. K., Dubey, N., Tiwari, S., & Tiwari, A. (2022, December). A Taxonomy towards fog computing Resource Allocation. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1-5. IEEE.

[8] Singh, N. K., Jain, A., Arya, S., Gonzales, W. E. G., Flores, J. E. A., & Tiwari, A. (2022, December). Attack Detection Taxonomy System in cloud services. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT), pp. 1-5. IEEE.

[9] Tiwari, A., & Garg, R. Reservation System for Cloud Computing Resources (RSCC): Immediate Reservation of the Computing Mechanism. *International Journal of Cloud Applications and Computing* (IJCAC), 12(1), 1-22 (2022).

[10] Tiwari, A., & Garg, R. Orrs Orchestration of a Resource Reservation System Using Fuzzy Theory in High-Performance Computing: Lifeline of the Computing World. *International Journal of Software Innovation* (IJSI), 10(1), 1-28 (2022).

[11] Agrawal S, Agrawal J. Survey on anomaly detection using data mining techniques. Procedia Comput Sci. 60 : 708-13 (2015).

[12] Tiwari, Ashish, and Ritu Garg. "A Optimized Taxonomy on Spot Sale Services Using Mathematical Methodology." *International Journal of Security and Privacy in Pervasive Computing* (IJSPPC) 14, No. 1, 1-21 (2022).

[13] Tiwari, A., & Sharma, R. M. OCC: A Hybrid Multiprocessing Computing Service Decision Making Using Ontology System. *International Journal of Web-Based Learning and Teaching Technologies* (IJWLTT), 16(4), 96-116 (2021).

[14] Tiwari, A., Sharma, V., & Mahrishi, M. Service adaptive broking mechanism using MROSP algorithm. In Advanced Computing, Networking and Informatics-Volume 2, pp. 383-391 (2014). Springer, Cham.

[15] Tiwari, A., Sharma, R. M., & Garg, R. Emerging ontology formulation of optimized internet of things (IOT) services with cloud computing. In Soft Computing: Theories and Applications, pp. 31-52 (2020). Springer, Singapore.

[16] Patcha A, Park J-M. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput Netw., 51(12) : 3448-70 2007.

[17] Jiang M, Cui P, Faloutsos C. Suspicious behavior detection: current trends and future directions. IEEE Intell Syst. 31(1) : 31-9 (2016).

[18] Kaur, R., Jain, A., & Kumar, S. Optimization classification of sunflower recognition through machine learning. Materials Today: Proceedings, 51, 207-211 (2022).

[19] Kumar, S., Kumari, B., & Chawla, H. Security challenges and application for underwater wireless sensor network. In Proceedings on International Conference on Emerg, Vol. 2, pp. 15-21, (2018, October).