Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1381–1391
DOI : 10.47974/JDMSC-1761

Authenticated key exchange protocol security of cloud services management using machine learning

Vani Agrawal *
Department of CSA
ITM University Gwalior
Madhya Pradesh
India

Nilesh Dubey †
Devang Patel Institute of Advance Technology and Research
Charotar University of Science and Technology
Gujarat 388421
India

Virendra Singh §
Department of Computer Application
Babu Banarsi Das University
Lucknow
Uttar Pradesh
India

Nepali Singla ‡
Department of CS
ABES Engineering College
Ghaziabad 201009
Uttar Pradesh
India

and

Syam Machinathu Parambil Gangadharan
The Home Depot
U.S.A.

* *E-mail:* vaniagrawal.cse@itmuniversity.ac.in (Corresponding Author)
† *E-mail:* nileshdubey.ce@charusat.ac.in
§ *E-mail:* virendsingh17@gmail.com
‡ *E-mail:* nepalishimla@gmail.com

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

Dinesh Goyal [#]
Department of CSE
Poornima Institute of Engineering and Technology
Jaipur
Rajasthan
India

Abstract

The reason for cloud-based confirmation is to shield organizations from programmers attempting to take classified data. Cloud validation permits approved clients across organizations and landmasses to safely get to data put away in the cloud with verification given through cloud-based administrations. Artificial intelligent (AI) permits organizations to empower the information to show the framework how to tackle the central issue with AI calculations and how to get better after some time. The present undertakings are assaulted with information. To drive better business decisions, they need to sort out it. Distributed computing is a huge term for all Data Science and Machine Learning Enthusiasts. It is far-fetched that you probably won't have run over it, even as a juvenile. The most important issue is that this type of security is needed for the cloud services. A clear explanation for this is that as the dataset develops, i.e., more models and features are added, the AI model ends up being more multifaceted. Internet Key Exchange (IKE) is a standard convention used to set up a safe and confirmed correspondence channel between two gatherings through a virtual private network (VPN). The convention guarantees security for VPN exchange, remote host and organization access.

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

Keywords: *Machine learning security, Cloud security organizations, Cloud authenticated system parameters, Cloud secure services, Security management, Cloud security simulation.*

[@] *E-mail:* **kr.sarvi91@gmail.com**
[#] *E-mail:* **dinesh8dg@gmail.com**

1. Introduction

Cloud administrations are at present a pattern in the IT business that has come to remain. These give a choice of putting away information on distant servers associated with the Internet. With cloud organizations, one can benefit from circulated processing, which offers a huge gathering of organizations to the client. These organizations range from server access, greater limit with regards to Big Data with better back-ups, and the ability to run excellent quality clever instruments for AI and BI by and large around the Internet as shown in the Figure 1. Besides, these organizations are certainly more reliable, speedier, sensible, more versatile, and adaptable to client needs. Clients can smooth out their costs through the capable use of these organizations [1][3]. Along these lines, fundamentally, in Cloud Computing, a client doesn't buy new server hardware yet rents it however lengthy needed. It is possible to rent circulated processing regardless, for single runs, which occasionally are several minutes [2]. Further, clients don't have to deal with the working frameworks and the united web benefits [5] the cloud specialist organizations oversee them all things considered. Nonetheless, in a long haul withinside the past, organizations needed to make an interest in various money in Machine Learning to get this benefit. AI required various frameworks, software engineers who had been familiar with ML, and records examination had been costly and there has been next to zero records to be needed to take care of those frameworks getting to know calculations! While this changed into now presently not that gigantic an arrangement for huge worldwide organizations, it changed into extremely intense for little and mid-degree organizations [7].

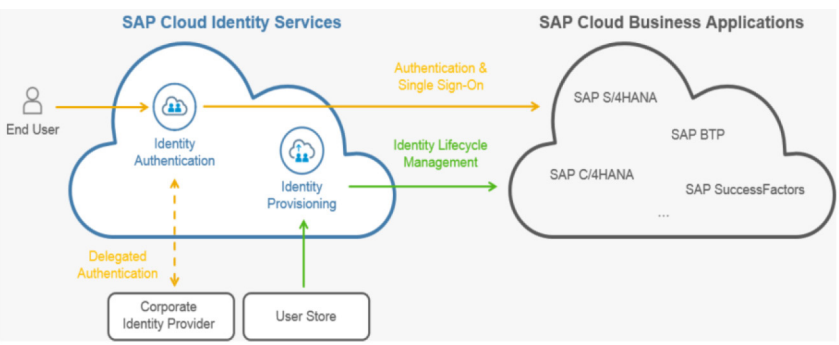

Figure 1

Cloud based Authentication security to ML

However, the acknowledgment and improvement of cloud contributions have made the entire part significantly simpler. Presently organizations can get section to Machine Learning calculations and innovation from a third-birthday celebration birthday festivity seller, made a few changes in accordance with their custom necessities are start getting the favors with a far more modest primer speculation. The first variant of IKE sets up secure correspondences diverts in two stages: stage 1 and stage 2.

In stage 1, a validated association between the host and client is laid out utilizing a pre shared key or a computerized endorsement. The objective is to get the correspondences that happen in stage 2. The Diffie-Hellman key trade calculation makes a protected verification correspondence channel. This advanced encryption strategy utilizes numbers raised to explicit powers to deliver decoding keys. The discussion ought to bring about meeting keys and one bidirectional SA [12]. Stage 1 works under one of two modes: fundamental mode or forceful mode. The fundamental mode comprises of the two players sending three two-way trades rising to six messages altogether. The initial two messages affirm encryption and validation calculations. The second arrangement of two messages begins a Diffie-Hellman key trade, where the two players give an irregular number. The third arrangement of messages confirms the personalities of each party. Forceful mode achieves a similar undertaking as the fundamental mode however does as such in only two trades of three messages. Though the primary mode safeguards the two players' characters by encoding them, the forceful mode doesn't.

2. Related Work

There are many clouds computing stages that give these web administrations to AI. The most well-known of these are IBM cloud, Azure, AWS and google cloud. These are the most established and most mature stages that give different items to Machine Learning going from regular language handling, administration bots, and, surprisingly, profound learning. So, in this article, we will look at every one of these distributed computing stages. Yet, before that, we should see the reason why cloud computing has become so significant in AI nowadays. The cloud administrations market is as of now overwhelmed by four central parts - Google, Microsoft, Amazon, and IBM since they offer the necessary web administrations for AI. These are IBM cloud, google cloud, Azure etc. These laid out stages expect to prepare all degrees of clients with

		Amazon Web Services (AWS), Amazon	Google Cloud Platform (GCP), Google	Azure, Microsoft
Type of service	**Feature/Facility**	**Tools**	**Tools**	**Tools**
Free trial for limited period	Servers and hours of usage	Yes, with restricted usage	Yes, with restricted usage	Yes, with restricted usage
Training modules for beginners	Tutorials & courses	Y	Y	Y
Data components	Data Storage	Y	Y	Y
	Dataset EDA	Y	Y	Y
Data ETL (Extract-Transform-Load)	ETL	Y	Y	Y
Data Analytics & Visualization	Dashboard/ Visualization	Y	Y	Y

Figure 2

Types of ML services provides by cloud CSPs

various Machine Learning apparatuses and Deep Learning. AWS or Amazon Web Services (2006), presented by Amazon, is one of the most perceived distributed computing stages for Machine Learning. This stage incorporates items like AWS machine learning security, IBM deep learning-based security for different Machine Learning necessities. To this end, Cloud Computing is so significant in Machine Learning This is the answer for some more modest and mid-level organizations that would rather not form, test, and carry out their own AI calculations without any preparation as shown in the Figure 2. These organizations can zero in on their center business and get esteem expansion from Machine Learning without expecting to become specialists. So, they get expanding benefits while diminishing their gamble of speculation which implies it's a mutually beneficial arrangement for all.

Likewise, Microsoft Azure (2010), as the name recommends is a help presented by Microsoft. It is a seriously well-known decision for AI and information investigation needs. This assistance incorporates items like IBM cloud, Azure cloud, AWS etc. Google Cloud or Google Cloud Platform GCP (2008) is a distributed computing stage given by Tech Giant Google. GCP offers different items for AI like Google Cloud, MI Cloud, NLP based cloud etc. for all Individual and Enterprise levels Machine Learning Projects [10]. At long last, IBM Cloud administration is given by IBM. It incorporates different cloud conveyance models that are public, private, and half-breed models. IBM Cloud offers different items for AI like AWS, azure, google cloud to help all Machine Learning needs [11].

3. Research Methodology

Cloud administrations are a decent choice for anybody hoping to prepare and convey memory-serious, complex Machine Learning/Deep Learning models. Cloud administrations are a savvy answer for both, individual clients as well as organizations [5,6]. At present, practically the distributed computing administrations are all utilized in enormous business server farms and their capability in an old brought together way. This methodology of planning has its advantages, i.e., Economy of scale and high sensibility, yet it has a few constraints. The greater part of the analysts is leaning towards utilizing expected assets to have cloud applications. This model of distributed computing which utilizes deliberate assets or a combination of both devoted and intentional assets is truly sensible and it suits such applications as logical processing. Notwithstanding, no matter what its benefits, this design has open exploration challenges also, which are heterogeneous assets on the board, and motivator plans for such engineering.

Perpetual assessment gives the idea that 75% of manager information experts itemized that they would require and use flowed figuring inside the nearby future [4,8]. According to Check Beccue's projection, the number of people using adaptable cloud applications will increase from 71 million to exceptionally approximately a billion by 2014. In prosperity regions, various affiliations, chiefs, and experts acknowledge that the disseminated figuring approach can similarly additionally foster organizations and benefits research [8-13]. The essential prevention in the speedy gathering of the cloud is the security nerves of the clients. While

Figure 3

Basic structure of Key exchange in ML

in view of the openness of current strategies for security the probabilities of wellbeing imperfections are diminished at this point, when worms and developers attack a structure, a tangle is made inside several hours as per the Figure 3.

It is fundamental that the applications and structures ought to be private and the system of safety should be important, developing and supportive. Trust and Privacy are a few other potential areas of examination in distributed computing. IKE might represent the accompanying difficulties: IKEv1 is defenseless against Bleichen bacher assaults, which get data about a gadget in light of the gadget's reaction to getting a changed ciphertext. IOS Cisco Systems actually support IKEv1. Involving IKEv2 in a few working frameworks (OS) may expect clients to make extra manual setups. For instance, in the event that IKE in Junos OS isn't expressly designed, Junos OS defaults to form 1 of IKE. There is likewise an opportunity that a firewall or an organization chairman could hinder IKEv2's UDP port, making a VPN quit working.

4. Proposed Methodical Structure

When carried out over a large scale, a lot of security initiatives, like hardware, programming, HR, and executive costs, are less expensive. The majority of cloud service providers replicate the data of their customers in various regions. This provides a degree of disaster recovery and raises information clear despair and freedom from structure dissatisfaction. Aside from that, the majority of the time, a cloud provider can successfully

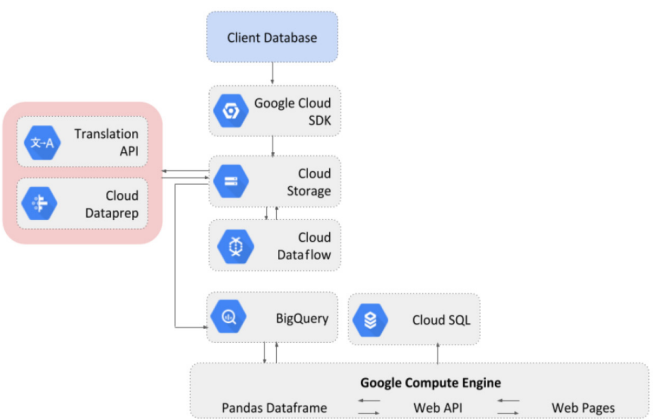

Figure 4

Working of ML services using cloud

enhance security assets for separating, traffic trimming, or encryption to enhance protection techniques.

The proposed technique utilizes the strategic guide which is iterated in two stages. It gives the reliance on past upsides of the guide so gives more irregularity. In this sort of guide, the contribution for the following emphasis is determined by a few parts of the result and some piece of the information. In this plan, the assailant can't foresee the grouping of the guide until he gets the data about a legitimate part of the values as per the strategies used in the Figure 4. There are 128 key bits that are taken from 1 to 128 bits.

The proposed interaction is made sense by following the calculation.

Proposed Algorithm Secure Process of Key exchange in ML computing services.

Input: For key exchange value image is taken as input.

Output: The optimized cloud resources are taken in ML by CSPs.

Begin:

For Encryption Process:

Find the value of 128 bits which is taken as input

Step1:

$$x_0 = \sum_{i=1}^{24} k_i / 2^i$$

$$x_0' = \sum_{i=25}^{48} k_i / 2^{i-24}$$

$$b_1 = \sum_{i=49}^{72} k_i / 2^{i-48}$$

$$b_2 = \sum_{i=73}^{96} k_i / 2^{i-72}$$

$$K_1 = \sum_{i=97}^{104} k_i$$

$$K_2 = \sum_{i=105}^{112} k_i$$

$$K_3 = \sum_{i=113}^{120} k_i$$

$$K_4 = \sum_{i=121}^{128} k_i$$

For the pixel value:

Find the new place of the pixel of the input image.

Step2:

$$y_{n+1} = r_1 * x_n(1 - x_n)$$

$$x_{n+1} = b_1 * y_{n+1} + (1 - b_1) * x_n$$

$$y'_{n+1} = r_2 * x'_n(1 - x'_n)$$

$$x'_{n+1} = b_2 * y'_{n+1} + (1 - b_2) * x'_n$$

$$Y' = float2int(y' * N)$$

In the newly find pixel place is I (X0; Y0)

For Modified value of the key rotation

Step3:

$$K_1' = K_1 \oplus (K_2 \vee K_3)$$

$$K_2' = K_2 \oplus (K_1 \& K_3)$$

$$K_3' = K_3 \oplus K_2 \oplus K_1$$

Step3.1:

Find the color value of the new pixel value I'(X', Y': R', G', B') for the pixel I'(X', Y': R, G, B).

$$R' = K_1' \oplus R \oplus K_4$$

$G' = K_2' \oplus G \oplus K_4$
$B' = K_3' \oplus B \oplus K_4$
$K_4 = K_4 \ll 1$
STEP 4
$K_1 = K_1'$
$K_2 = K_2'$
$K_3 = K_3'$
$B' = K_3' \oplus B \oplus K_4$
End.

5. Discussion and Conclusion

This paper offers a complete assessment of what Cloud Services are, why those are important for AI and Machine Learning requirements, and shows a method to deciding on a carrier in case you are an amateur. Although maximum of those companies offer systems for general-cause AI and ML desires, an amateur nonetheless desires to select a platform that is straightforward to use, calls for no Cloud know-how to set up & run, and gives higher guide and gear for Machine Learning inclusive of NLP, chatbots, or carrier bots in addition to Neural Networks for Deep Learning. IKE offers a few advantages for IPsec design, including programmed exchange and confirmation, hostile to replay administrations, certificate authority support and the capacity to change encryption keys during an IPsec meeting.

References

[1] Meena, G., & Choudhary, S. Biometric authentication in internet of things: A conceptual view. *Journal of Statistics and Management Systems*, 22(4) (2019).

[2] Tiwari, A., Kumar, S., Baishwar, N., Vishwakarma, S. K., & Singh, P. (2022, September). Efficient Cloud Orchestration Services in Computing. In Proceedings of 3rd International Conference on Machine Learning, Advances in Computing, Renewable Energy and Communication: MARC 2021 (pp. 739-746). Singapore: Springer Nature Singapore.

[3] R. Arun Raj, S.N. George, and P.P. Deepthi. An expeditious chaos based digital image encryption algorithm. In Recent Advances in Information Technology (RAIT), 2012 1st International Conference on (2012).

[5] David M. Curry. Practical application of chaos theory to systems engineering. Procedia CS (2012).

[6] Wenping Guo. A new digital image scrambling encryption algorithm based on chaotic sequence. In Computer Research and Development (ICCRD), 2011 3rd International Conference on, volume 1 (2011).

[7] Dhanda, S. S., Singh, B., & Jindal, P. Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks. *Journal of Interdisciplinary Mathematics*, 23(2) (2020).

[8] Yue Sun and Guangyi Wang. An image encryption scheme based on modified logistic map. In Chaos-Fractals Theories and Applications (IWCFTA), 2011 Fourth International Workshop on (2011).

[9] Tiwari, A., Sah, M. K., & Malhotra, A. Effective service Utilization in Cloud Computing exploitation victimisation rough pure mathematics as revised ROSP. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-6). IEEE (2015, September).

[10] L. Kocarev and S. Lian. Chaos-based Cryptography: Theory, Algorithms and Applications. Studies in Computational Intelligence. Springer (2011).

[11] Tiwari, A., & Garg, R. A Optimized Taxonomy on Spot Sale Services Using Mathematical Methodology. *International Journal of Security and Privacy in Pervasive Computing* (IJSPPC), 14(1), 1-21 (2022).

[12] B Sivakumar. Chaos theory in hydrology: important issues and interpretations. *Journal of Hydrology*, (2005).

[13] 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.

[14] Mittal, G., Kumar, S., & Kumar, S. Novel public-key cryptosystems based on NTRU and algebraic structure of group rings. *Journal of Information and Optimization Sciences*, 42(7) (2021).

[15] Tiwari, A., & Garg, R. Eagle Techniques In Cloud Computational Formulation. International *Journal of Innovative Technology and Exploring Engineering*. Issue (9s), pp. 422-429, (2019).

[16] 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).

[17] Chouhan, A., Tiwari, A., Diwaker, C., & Sharma, A. Efficient Opportunities and Boundaries towards Internet of Things (IoT) Cost Adaptive Model. In 2022 IEEE Delhi Section Conference (DELCON) (pp. 1-5). IEEE (2022, February).

[18] Tiwari, A., & Garg, R. Adaptive Ontology-Based IoT Resource Provisioning in Computing Systems. *International Journal on Semantic Web and Information Systems* (IJSWIS), 18(1), 1-18 (2022).

[19] Tiwari, A., & Garg, R. ACCOS: A Hybrid Anomaly-Aware Cloud Computing Formulation-Based Ontology Services in Clouds. In ISIC, pp. 341-346, (2021).

[20] Kamble, S., Saini, D. K. J., Kumar, V., Gautam, A. K., 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).

[21] Tiwari, A., & Sharma, R. M. A Skywatch on the Challenging Gradual Progression of Scheduling in Cloud Computing. In Applications of Computing, Automation and Wireless Systems in Electrical Engineering, pp. 531-541 (2019). Springer, Singapore.

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

[23] 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).

[24] 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).

[25] 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).

[26] 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).