Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

FOG-TO-CLOUD COMPUTING FOR CLOUD STORAGE USING MAC AND HMAC

Shivaleela H

Assistant professor

Dept. Of Computer Science

Government First Grade College For Women

Jamakhandi 587301, Bagalakot Dist, Karnataka.

ABSTRACT

As a consequence of the growth of the IoT, fog-to-cloud computing has arisen as a viable new approach. The cloud specialist organization (CSP) isn't the main player in haze to-distributed computing; versatile sinks and mist hubs are likewise required. Subsequently, the reviewing of information trustworthiness in haze to-distributed storage will appear to be unique than it does in additional regular mists. Tian et al. have as of late stepped up to the plate and construct a public inspecting framework for the change from haze to distributed computing. Bilinear mapping, proof of knowledge, and other complex public key cryptography techniques are central to their strategy.It becomes exceedingly inefficient. In this research, we use MAC and HMAC, two widely-used private key cryptography algorithms, to create a standardized, more effective auditing system. We provide a tangible example of our auditing system by using MAC and HMAC. Finally, both theoretical research and experimental findings confirm that our suggested method is more cost-effective in terms of both data transmission and processing.

1. INTRODUCTION

Since its introduction by Bonomi et al. in 2012 [6], fog computing has become a standard method for many different types of industrial domains that rely on IOT devices[15], [16], [19], [32]. Fog computing nodes, which serve as a bridge between Internet of Things (IoT) devices and clouds, are equipped with basic computation, storage, and resources to meet the needs of data preparation and transfer. For this reason, certain resource-constrained, enormous scope modern applications are starting to see the haze to-distributed computing engineering as an engaging option for information capacity.Since its introduction by Bonomi et al. in 2012 [6], fog computing has become a standard method for many different types of industrial domains that rely on IOT devices[15], [16], [19], [32]. Fog computing nodes, which serve as a bridge between Internet of Things (IoT) devices and clouds, are equipped with basic computation, storage, and resources to meet the needs of data preparation and transfer. For this reason, certain resource-constrained, the fog-to-cloud computing architecture is starting to be recognized by large-scale industrial applications as a desirable option for data storage.

Some of the same classical difficulties that have plagued conventional clouds also affect fog-to-cloud architectures.How to guarantee data integrity in a cloud storage service is a common worry. I'll explain why. Some CSPs can attempt to hide the fact that vital information stored in IoT gadgets or fog nodes has been lost or damaged as a result of various forms of assault [25]. like a result, much like in classic cloud computing, the advancement of successful evaluating devices for safe information stockpiling in haze to-distributed computing is profoundly required and critical.

While various private and public auditing techniques have been provided for conventional cloud storage over the last few years [12, [22], [25], [26], [31],[33], Fog-to-cloud computing is irrelevant to none of them. [23], [24]. The _rst is that users (or data owners) should not obtain this data and produce appropriate authenticators before outsourcing, since this is unnecessary due to the distributed nature of IOT data generation. Another, more critical issue is that current reviewing arrangements do exclude haze registering hubs, which are fundamental parts of mist to-distributed computing on the grounds that to their capacity to successfully process and quickly send for enormous scope IOTdata. Subsequently, new examining instruments to guarantee information uprightness for haze to-distributed computing should be grown right away. Ongoing work by Tian et al. [The initial attempt to fill this void is [23]. Utilizing bilinear planning and the supposed tag-changing technique, they fostered a public examining framework that safeguards clients' obscurity.The performance of their strategy was also analyzed theoretically and thoroughly tested.

In public auditing schemes, it is common practice to delegate responsibility for ensuring users' data is accurate to a trusted third-party auditor (TPA) who may have access to superior expertise in auditing as well as more computing resources. It's important to remember, too, that public auditing systems are notoriously inefficient compared to their private sector counterparts. Time spent proving, confirming, and outsourcing in a public auditing system may be hundreds, if not thousands, of times longer than in a private scheme, as Zhang et al. shown in [33]. Hence, we think the private examining framework might be more famous in specific circumstances where productivity is being looked for, especially for the asset obliged portable sinks in haze to-distributed computing. Therefore, it is crucial to provide effective private reviewing methods for the relocation from distributed computing to haze.

This paper is an endeavor to head down that path. Message validation code (Macintosh) [14] and homomorphic Macintosh (HMAC) [2, [8], [10]approaches are fundamental cryptographic building blocks, and we present a novel auditing system based on these techniques. Data blocks saved in CSP are verified for integrity using the HMAC algorithm, while the Macintosh technique is utilized for transmission between portable sinks and haze hubs. Since a shared secret key is required for the meetings in Macintosh or HMAC for creating or approving the labels, this approach is not appropriate for presenting TPA.

We likewise give an unmistakable illustration of the framework in real life by showing how to carry out the hash-based Macintosh strategy depicted in [14] and the able HMAC strategy created by Agrawal and Boneh.

We likewise think about the introduction of our proposed system to that of Tian et al. as well as to two normally involved cloud assessment procedures in [20] and [18].The trial information exhibits that our framework is more practical and productive in its calculations than the one created by Tian et al. In addition, our protocol is superior to the two techniques in [18, 20] since it may be used for fog-to-cloud computing.

Some of the same classical difficulties that have plagued conventional clouds also affect fog-to-cloud architectures.How to guarantee data integrity in a cloud storage service is a common worry. I'll explain why. Some CSPs can attempt to hide the fact that vital information stored in IoT gadgets or fog nodes has been lost or damaged as a result of various forms of assault [25]. like a result, much like in classic cloud computing, the development of effective auditing tools for safe information capacity in haze to-distributed computing is exceptionally required and crucial.

While various private and public auditing techniques have been provided for conventional cloud storage over the last few

years [12, [22], [25], [26], [31],[33], Fog-to-cloud computing is irrelevant to none of them. [23], [24]. The _rst is that users (or data owners) should not obtain this data and produce appropriate authenticators before outsourcing, since this is unnecessary due to the distributed nature of IOT data generation. Another, more critical issue is that current reviewing arrangements do exclude haze registering hubs, which are fundamental parts of mist to-distributed computing on the grounds that to their capacity to successfully process and quickly send for enormous scope IOTdata. Subsequently, new examining instruments to guarantee information uprightness for haze to-distributed computing should be grown right away. Ongoing work by Tian et al. [The initial attempt to fill this void is [23]. Utilizing bilinear planning and the supposed tag-changing technique, they fostered a public examining framework that safeguards clients' obscurity. The performance of their strategy was also analyzed theoretically and thoroughly tested.

In public auditing schemes, it is common practice to delegate responsibility for ensuring users' data is accurate to a trusted third-party auditor (TPA) who may have access to superior expertise in auditing as well as more computing resources. It's important to remember, too, that public auditing systems are notoriously inefficient compared to their private sector counterparts. Time spent proving, confirming, and outsourcing in a public auditing system may be hundreds, if not thousands, of times longer than in a private scheme, as Zhang et al. shown in [33]. Hence, we think the private examining framework might be more famous in specific circumstances where productivity is being looked for, especially for the asset obliged portable sinks in haze to-distributed computing. Consequently, it is essential to develop effective private evaluating strategies for the change from distributed computingto fog.

This paper is an endeavor to head down that path. Message validation code (Macintosh) [14] and homomorphic Macintosh (HMAC) [2, [8], [10]approaches are fundamental cryptographic building blocks, and we present a novel auditing system based on these techniques. Information blocks saved in CSP are confirmed for uprightness utilizing the HMAC calculation, though the Macintosh technique is utilized for transmission between portable sinks and haze hubs. Since a shared secret key is required for the meetings in Macintosh or HMAC for creating or approving the labels, this approach is not appropriate for presenting TPA.

We likewise give an unmistakable illustration of the framework in real life by exhibiting how to carry out the hash-based Macintosh strategy depicted in [14] and the fruitful HMAC strategy created by Agrawal and Boneh.

Furthermore, we contrast the presentation of our proposed framework with that of Tian et al. also, two normal strategies for cloud reviewing in [20] and [18]. Theexploratory information shows that our framework is more financially savvy and proficient in its calculations than the one created by Tian et al. In addition, our protocol is superior to the two techniques in [18, 20] since it may be used for fog-to-cloud computing.

2. LITERATURESURVEY

Proof of Retrievability (PoR) was proposed by Jues and Kaliski [13], one of the early endeavors tocontemplate the security of information in the cloud.Data integrity in PoR may be guaranteed by combining error-correcting coding with random data block checks. However, this method can only handle a small handful of checks. At the same time, Ateniese et al. [3] suggested RSA-homomorphic authenticators based on proven data possession (PDP), which can accommodate an infinite number of challenges and public auditing. There have since been several publications that aim

to enhance the effectiveness of communication [4, 7, 11, 20].

Other studies [12, 22], 26], and 28] have pondered the possibility of dynamic updates to PDP systems. Authenticated data structures are becoming more used in public auditing systems as a means of supporting data dynamics. In 2011, Wang et al. [26] proposed Merkle-hash-tree-based public examining for live information.To achieve information elements, Zhu et al. later, they presented a brand-new data structure that they referred to as an index hash table [34]. Tian et al. in 2017 [22] suggested a two-layered information structure termed a unique hash table to support both continuous information updating and public examination. A unique structure that combines a position array with a doubly linked information table to provide dynamic data was developed around the same time by Shen et al. [21]. While there are productive methodologies portrayed for regular distributed storage, just a little subset of them might be promptly stretched out to achieve proficient and safe confirmation for information capacity in haze to-cloud based IoT circumstances.

Here are the two primary explanations. To start, in the haze to-cloud situation, information are frequently made by various IoT gadgets as opposed to information proprietors. Second, in the mist to-cloud situation, certain new elements, like haze hubs, are made and assume pivotal parts for handling and transmission. However, they are ignored by the prevalent model of cloud storage. As a result, this void in the public auditing scenario was addressed by Kashif and Mohammed [18] and Tian et al. [23] using methodologies that complement one another. The two articles neglect the best confidential key examining frameworks. Concerning haze registering, we bring up that Wu et al., in their new paper [27], proposed a mist registering empowered mental organization capabilities virtualization approach for a data driven future Web, and they likewise planned a correspondence conspire between the haze hubs and the future Web Hubs for the sending system.

[1] **J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, ‘‘Charm: A framework for quickly prototyping cryptosystems," Journal of Cryptographic Engineering, vol. 3, no. 2, June 2013, pp. 111–128.**

In this article, Charm, a modular framework for quickly creating secure cryptographic prototypes, is presented.With Charm, you have access to a large library of reusable code, a framework for creating interactive protocols, and support for modular construction of cryptographic building pieces, all of which are designed to facilitate the creation of new protocols. Our framework also offers a suite of specific tools for facilitating communication between various cryptosystems. We used Charm to create over 40 different kinds of cryptographic systems, including several that, to the best of our knowledge, have never been developed before. Our modular design is described in this work, and it has an integrated benchmarking module for evaluating the efficiency of Charm primitives in relation to preexisting C implementations. We demonstrate that our methods often lead to a reduction in code size by an order of magnitude, while still causing an acceptable performance hit. Finally, we have built up a sizable, active user base for the Charm framework since making it accessible to the research community at no cost.

[2] S. Agrawal and D. Boneh, ‘‘Homomorphic MACs: MAC-based integrity for network coding, in Lecture Notes in Computer Science, vol. 5536, Applied Cryptography and Network Security. 2009, Springer, Berlin, Germany, pp. 292-305.

Evidence suggests that network coding may increase both network capacity and resiliency. Data integrity cannot be verified using conventional MACs and checksums due to packet modification by intermediary nodes. Furthermore, since a single errant node might flood the network with wrong parcels and keep the recipient from accurately interpreting the bundles, network-coded frameworks are truly vulnerable to contamination assaults. There have been proposition for signature strategies to forestall these assaults, but they are frequently

excessively delayed for per-bundle online uprightness.

In this paper, we present a homomorphic Macintosh for checking the validness of organization encoded information. In the event that your framework utilizes network coding, our homomorphic Macintosh might be utilized as an immediate substitution for more seasoned Macintoshes like HMAC.

[3] G. Ateniese, R. Burns, R. Curtmola, Joseph Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted storage,'' in Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA, 2007, pp. 598–609.

We give a worldview to demonstrated information ownership (PDP) that empowers a client to confirm that an untrusted server holds information without really getting the information from the server. To eliminate I/O expenses, the model gives probabilistic evidences of proprietorship by haphazardly choosing gatherings of blocks from the server.The client always has a certain amount of information available to confirm the evidence. The test/reaction conventionkeeps network traffic to a minimum by constantly sending out just a tiny quantity of data. This means that the PDP model for remote data verification is suitable for use with big data sets stored in a dispersed environment.

We provide two provably-secure PDP schemes that outperform prior solutions while also providing better efficiency than methods achieving lesser guarantees. In instance, unlike with other storage methods, server overhead is very minimal (or constant) regardless of the amount of data being stored. Our implementation's experimental results demonstrate the viability of PDP and show that disk I/O, rather than cryptographic computing, limits PDP's speed.

[4] G. Ateniese, S. Kamara, and J. Katz, ‘‘Proofs of storage from homomorphic identification methods, Berlin, Germany: Springer, Advances in Cryptology, 2009, pp. 319–333.

Proofs of storage (PoS) are intelligent conventions empowering a client to check in the event that a server is being honest about its record stockpiling.It has been shown in the past that any homomorphic linear authenticator (HLA) may be used to build proofs of storage. The latter are signature/message authentication techniques in which every linear combination of messages may have a "tag" created by homomorphically combining the "tags" of several messages.

To create public-key HLAs, we present a framework that may be used to any identifying protocol that satisfies specific homomorphic features. Next, we show how to change over any open key HLA into an unreservedly obvious PoS with correspondence intricacy that is free of record size and takes a boundless number of confirmations. To demonstrate our modifications, we apply them to a variation of a Shoup identification protocol, resulting in the first factoring-based PoS with unlimited usage (in the random oracle model).

[5] A. F. Barsoum and M. A. Hasan, In cloud computing systems, "provable multicopy dynamic data possession," IEEE Trans. Inf. Forensics Security, March 2015, volume 10, issue 3, pages 485–497.

More and more businesses are choosing to store their data with external CSPs located in the cloud. By paying a monthly subscription per gigabyte of data stored, customers get access to the CSP's storage infrastructure for almost limitless data storage and retrieval. A few clients might decide to have their data put away in various duplicates across a few server farms to further develop versatility, accessibility, and strength. The more clients maintain that their CSP should keep, the more cash they'll need to pay.To this end, it is essential that consumers have confidence that the CSP is securely archiving all copies of customer data as per the terms of the service agreement, and that these copies accurately reflect the most up-to-date customer edits. Highlights of the guide based demonstrated multicopy dynamic information

ownership (MB-PMDDP) move toward proposed in this work incorporate the accompanying. Notwithstanding the advantages referenced above, it additionally works with the reevaluating of dynamic information by permitting block-level tasks like block change, inclusion, cancellation, and affix, and in this manner guaranteeing that main approved clients approach the record copies set aside by the CSP, thus supporting clients that the CSP isn't cheating by taking care of less copies.We evaluate the proposed MB-PMDDP technique against a benchmark derived by enhancing preexisting verifiable ownership of dynamic single-copy protocols. Experiments conducted on a commercial cloud infrastructure corroborate the theoretical theory. We also demonstrate the scheme's resistance to collaborating servers and offer methods for spotting tainted copies.

[6] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its function in the Internet of Things, in Proceedings of the First MCC Workshop on Mobile Cloud Computing, New York, NY, USA, 2012, pp. 13–16.

Haze Registering considers another class of utilizations and administrations by bringing the Distributed computing model to the organization's outskirts. The following are some features of fog: Low latency, location awareness, mobility, a large number of nodes, wireless access supremacy, streaming and real-time applications, extensive geographic dispersion, and all of the above and g) heterogeneity. In this review, we suggest that the Haze's previously mentioned properties make it an optimal host for an assortment of fundamental IoT administrations and applications, including Associated Vehicles, Shrewd Lattices, Brilliant Urban communities, and WSANs overall.

3. PROBLEM STATEMENT

It was Jues and Kaliski [13] who first proposed the term. By doing random checks on data blocks in addition to using error-correcting code, data integrity may be guaranteed in PoR. However, this method can only handle a small handful of checks. Concurrently, Atniese et al. [3] developed RSA-homomorphic authenticators based on proven data possession (PDP), which allows for an endless number of challenges and public auditing.

There have since been several publications that aim to enhance the effectiveness of communication [4, 7, 11, 20]. Other studies [12, 22], 26], and 28] have pondered the possibility of dynamic updates to PDP systems. Authenticated data structures are becoming more used in public auditing systems as a means of supporting data dynamics. In 2011, Wang et al. [26] proposed Merkle-hash-tree-based public auditing for live data. To achieve information elements, Zhu et al. later, they presented a brand-new data structure that they referred to as an index hash table [34]. A two-layered information structure called a unique hash table was proposed by Tian et al. in 2017 [22] to give both public examining and continuous information refreshing. A comparative creative design, utilizing a doubly connected data table and an area cluster, was introduced around the same time [21] by Shen et al.

While there are productive methodologies portrayed for regular distributed storage, just a little subset of them might be promptly stretched out to achieve proficient and safe confirmation for information capacity in haze to-cloud based IoT circumstances. The two primary explanations are as follows: To start, in the haze to-cloud situation, information are frequently made by various IoT gadgets as opposed to information proprietors. Second, in the mist to-cloud situation, certain new substances, like haze hubs, are made and assume vital parts for handling and transmission.However, they are ignored by the prevalent model of cloud storage.

As a result, this void in the public auditing scenario was addressed by Kashif and Mohammed [18] and Tian et al. [23] using methodologies that complement one another. Both articles overlook the most effective private key auditing systems.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

3.1 Limitation of system

Outsourced information was not subjected to Attribute Based Encryption or any other kind of data audits by the system. The absence of Identity-Based Encryption makes the system less secure.

4. PROPOSEDSYSTEM

The suggested system makes an effort in this approach. Message authentication code (MAC) [14] and homomorphic MAC (HMAC) [2, 8]_[10] methods are fundamental cryptographic building blocks, and we present a novel auditing system based on these approaches. Portable sinks and haze hubs utilize the Macintosh strategy for information move, while blocks of information saved in CSP are confirmed utilizing the HMAC calculation.Since a shared secret key is required for the meetings in Macintosh or HMAC for creating or approving the labels, this process is inappropriate for presenting TPA. We also present a practical demonstration of the system by using the hash-based MAC approach described in [14] and the efficient HMAC technique developed by Agrawal and Boneh.

4.1 Advantages

CANCELLATION OF DATA. DUAL GOAL OF DYNAMIC UPDATE AND REPLAY ATTACK PREVENTION. Improve the safety of data sent from afar with the help of Data Auditing and Recovery Methods.

5. SYSTEM ARCHITECTUR

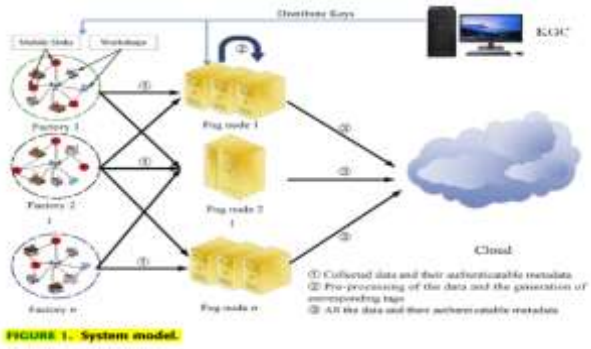


FIGURE 1. System model.

6. IMPLEMENTATION

6.1 SENDER (OWNER)

Before a sender may take any actions in this module, he must first sign up and get permission to do so. Once authorized, the sender may upload a file that includes a trapdoor and then use those controls to make changes, delete the file, validate it, or restore it.

6.2 CSP

In this section, CSP will provide access to both the sender and the recipient. And check out the cloud file you just uploaded, as well as any potential threats it may have. Examine the data with its encryption removed and its associated secret keys and transactions shown.

6.3 RECEIVER (USER)

After logging in, users may search for files using keywords, request access to the secret key, and then download the file from the cloud if they have the necessary decryption rights.

6.4 FOG

Accesses and examines all user requests for decryption permissions on files, as well as the transactions and information associated with those requests.

6.5 KGC

The private key is generated using this module's private key generator. In doing so, it creates two distinct keys, such as pkey1 and pkey2. Different users may access the same file and see all of the produced secret keys and associated transactions using their own unique generated key.

7. ALOGORITHMS USED

7.1. HOMOMORPHIC MAC

After verifying the accuracy of the newly computed tag t for a message v, which is actually a (n + s)-dimensional vector in any finite field Fq, "legitimate" users can recompute a new tag on the combined message using a homomorphic message authentication code (MAC) system. A (q, n, s) homomorphic MAC scheme's four PPT algorithms

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

are formalized as follows: HMAC-KeyGen, HMAC, HCombine, and HVerify.

The HMAC-KeyGen:

This algorithm creates and returns a secret key K based on the input λ.

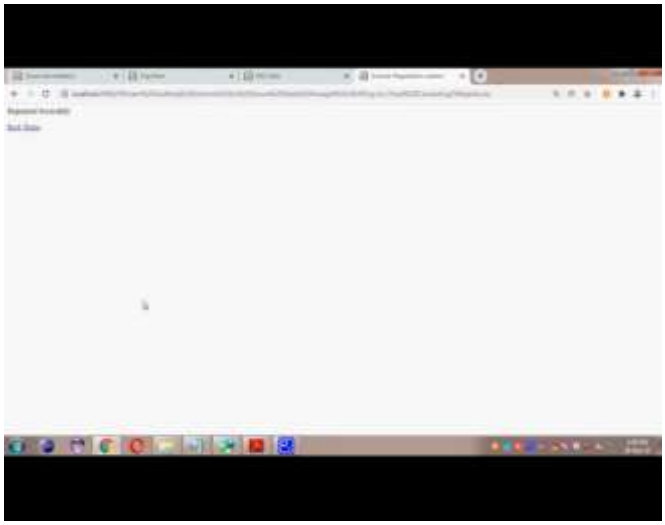
HMAC : Here we use the identifier id, the secret key K, the scalar j ∈ [s] and the augmented vector v to show that v ∈ F n+s q is the j-th basis vector of the vector space id.For v, the result of this procedure is a label T.

HCombine : Given'(' < s) constants r1,...,r' Fq, vectors v1,...,v' F n+s q, and tags T1,...,T', this strategy returns a label T for the consolidated vector y:= P' i=1 rivi F n+s q.

HVerify: This method returns either 0 (reject) or 1 (accept) for the contributions of a mystery key K, an identifier id, a vector y F n+m q, and a label T. In order for Tj = HMAC(K, id, vj, j) to be accurate, it must be true that 1 HMAC(K, id, vj, j) for any mystery key K, r1,.., r' Fq.Verify

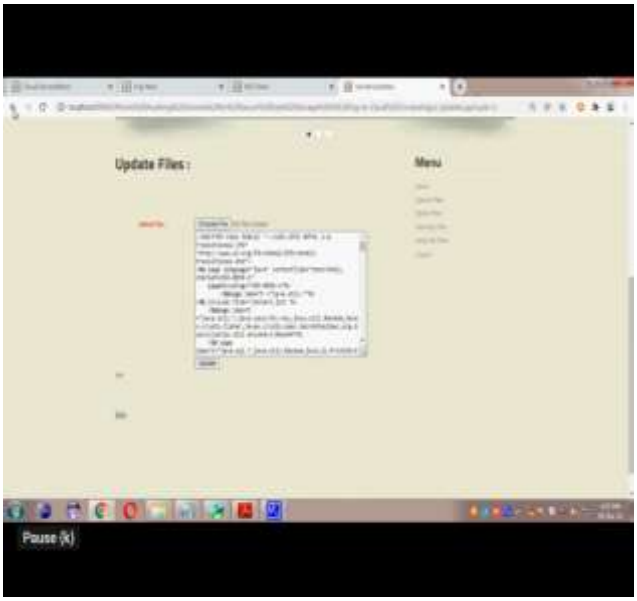
$$\times \left(K, id, \sum_{j=1}^{\ell} r_j v_j, \texttt{HCombine}\left(\left\{ (r_j, v_j, T_j)_{j=1}^{\ell} \right\} \right) \right)$$

Signatures on whatever vector space it chooses, but cannot provide a valid triple (id, y, T) in which id is either novel or identical to some identifier idi for which it has gotten the associated signature but y does not belong to the space described by idi.

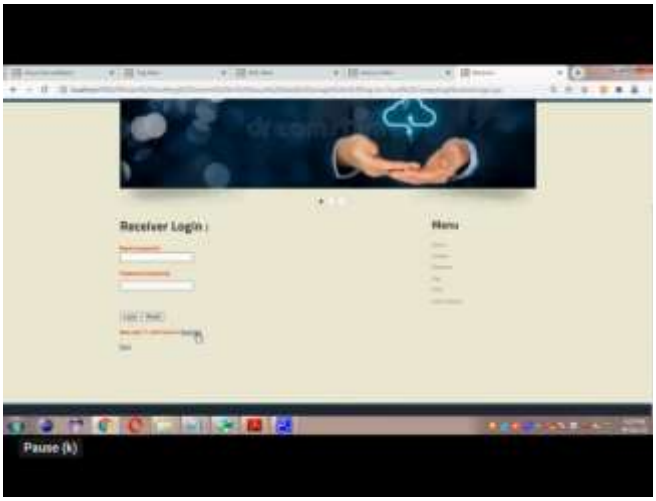


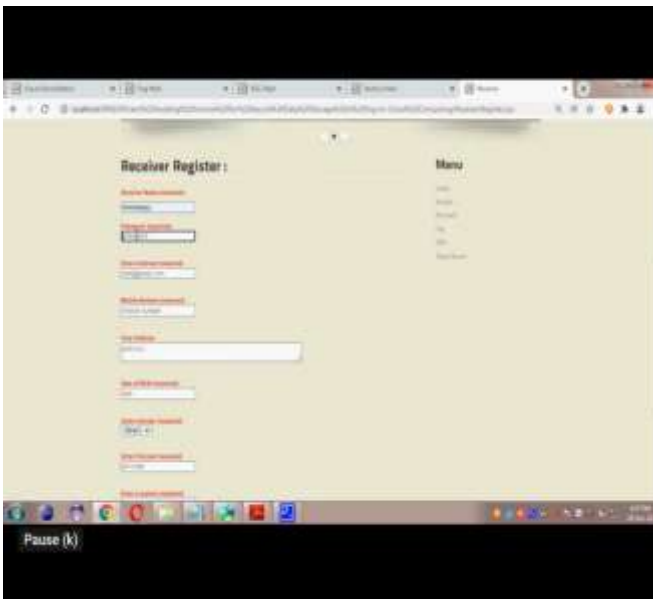
8. OUTPUT RESULTS

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

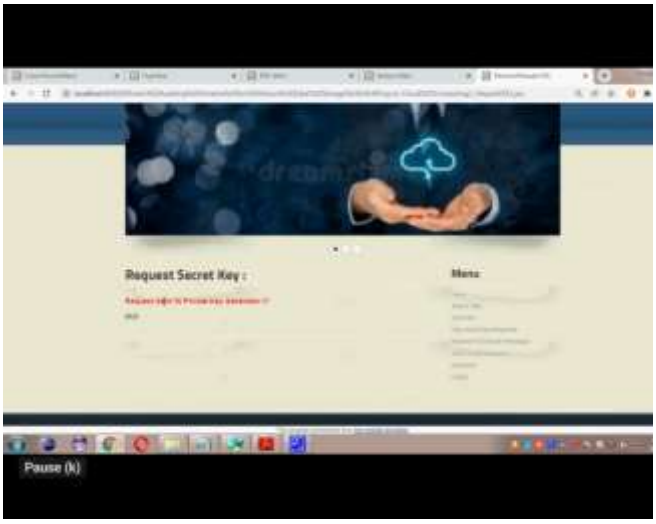


Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023





Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023



9. CONCLUSION

An effective auditing mechanism for the transition from fog to cloud environments is proposed in this research. As far as both correspondence and processing proficiency, our methodology is obviously better than that introduced by Tian et al., regardless of the way that it isn't expected for public evaluating.The computing efficiency is shown by the simulation results. We think our suggested solution would be a great option for fog-to-cloud computing's safe data storage.

10. REFERENCES

[1] V. Subrahmanian and S. Kumar, ``Predicting human behavior: The next frontiers," *Science*, vol. 355, no. 6324, p. 489, 2017.

[2] H. Lauw, J. C. Shafer, R. Agrawal, and A. Ntoulas, ``Homophily in the digital world: A LiveJournal case study," *IEEE Internet Comput.*, vol. 14, no. 2, pp. 15_23, Mar./Apr. 2010.

[3] M. A. Al-Garadi, K. D. Varathan, and S. D. Ravana, ``Cybercrime detection n online communications: The experimental case of cyberbullying detection in the Twitter network," *Comput. Hum. Behav.*, vol. 63, pp. 433_443, Oct. 2016.

[4] L. Phillips, C. Dowling, K. Shaffer, N. Hodas, and S. Volkova, ``Using social media to predict the future: A systematic literature review," 2017, *arXiv:1706.06134*. [Online]. Available: https://arxiv.org/abs/1706.06134

[5] H. Quan, J. Wu, and Y. Shi, ``Online social networks & social network services: A technical survey," in *Pervasive Communication Handbook*. Boca Raton, FL, USA: CRC Press, 2011, p. 4.

[6] J. K. Peterson and J. Densley, ``Is social media a gang? Toward a selection, facilitation, or enhancement explanation of cyber violence," *Aggression Violent Behav.*, 2016.

[7] BBC. (2012). *Huge Rise in Social Media*. [Online]. Available: http://www.bbc.com/news/uk-20851797

[8] P. A.Watters and N. Phair, ``Detecting illicit drugs on social media using automated social media intelligence analysis (ASMIA)," in *Cyberspace Safety and Security*. Berlin, Germany: Springer, 2012, pp. 66_76.

[9] M. Fire, R. Goldschmidt, and Y. Elovici, ``Online social networks: Threats and solutions," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 2019_2036, 4th Quart., 2014.

[10] N. M. Shekokar and K. B. Kansara, ``Security against sybil attack in social network," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, 2016, pp. 1_5.

[11] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonçalves, A. Flammini, and F. Menczer, ``Detecting and tracking political abuse in social media," in *Proc. 5th Int. AAAI Conf. Weblogs Social Media*, 2011, pp. 297_304.

[12] A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, ``PhishAri: Automatic realtime phishing detection on Twitter," in *Proc. eCrime Res. Summit (eCrime)*, Oct. 2012, pp. 1_12.

[13] S. Yardi*et al.*, ``Detecting spam in a Twitter network," *First Monday*, Jan. 2009. [Online]. Available: https://_rstmonday.org/ article/view/2793/2431

[14] C. Yang, R. Harkreader, J. Zhang, S. Shin, and G. Gu, ``Analyzing spammers' social networks for fun and pro_t: A case study of cyber criminal ecosystem on twitter," in *Proc. 21st Int. Conf. World Wide Web*, 2012, pp. 71_80.

[15] G. R. S.Weir, F. Toolan, and D. Smeed, ``The threats of social networking: Old wine in new bottles?" *Inf. Secur. Tech. Rep.*, vol. 16, no. 2, pp. 38_43, 2011.

[16] M. J. Magro, ``A review of social media use in e-government," *Administ. Sci.*, vol. 2, no. 2, pp. 148_161, 2012.

[17] M. Dadvar, D. Trieschnigg, R. Ordelman, and F. de Jong, ``Improving cyberbullying detection with user context," in *Advances in Information Retrieval*. Berlin, Germany: Springer, 2013, pp. 693_696.

[18] Y. Chen, Y. Zhou, S. Zhu, and H. Xu, ``Detecting offensive language in social media to protect adolescent online safety," in *Proc. Int. Conf Privacy, Secur., Risk Trust (PASSAT)*, Sep. 2012, pp. 71_80.

[19] V. S. Chavan and S. S. Shylaja, ``Machine learning approach for detection of cyber-aggressive comments by peers on social media network," in *Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI)*, Aug. 2015, pp. 2354_2358.

[20] W. Dong, S. S. Liao, Y. Xu, and X. Feng, ``Leading effect of social media for _nancial fraud disclosure: A text mining based analytics," in *Proc. AMCIS*, San Diego, CA, USA, 2016.

[21] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, ``FRAppE: Detecting malicious Facebook applications," in *Proc. 8th Int. Conf. Emerg. Netw. Exp. Technol.*, 2012, pp. 313_324.

[22] S. Abu-Nimeh, T. Chen, and O. Alzubi, ``Malicious and spam posts in online social networks," *Computer*, vol. 44, no. 9, pp. 23_28, Sep. 2011.

[23] B. Doerr, M. Fouz, and T. Friedrich, ``Why rumors spread so quickly in social networks," *Commun. ACM*, vol. 55, no. 6, pp. 70_75, Jun. 2012.

[24] J. W. Patchin and S. Hinduja, *Words Wound: Delete Cyberbullying and Make Kindness Go Viral*. Golden Valley, MN, USA: Free Spirit Publishing, 2013.

[25] J. Cheng, C. Danescu-Niculescu-Mizil, and J. Leskovec, ``Antisocial behavior in online discussion communities," in *Proc. 9th Int. AAAI Conf. Web Social Media*, Apr. 2015.

[26] S. Liu, J. Zhang, and Y. Xiang, ``Statistical detection of online drifting Twitter spam: Invited paper," in *Proc. 11th ACM Asia Conf. ComputCommun. Secur.*, 2016, pp. 1_10.

[27] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, ``Twitter spammer detection using data stream clustering," *Inf. Sci.*, vol. 260, p. 64_73, Mar. 2014.

[28] M. Jiang, S. Kumar, V. S. Subrahmanian, and C. Faloutsos, ``KDD 2017 tutorial: Data-driven approaches towards malicious behavior modeling," *Dimensions*, vol. 19, p. 42, 2017.

[29] S. Y. Jeong, Y. S. Koh, and G. Dobbie, ``Phishing detection on Twitter streams," in *Proc. Paci_c_Asia Conf. Knowl. Discovery Data Mining*. Cham, Switzerland: Springer, 2016, pp. 141_153.

[30] I. Frommholz, H. M. Al-Khateeb, M. Potthast, Z. Ghasem, M. Shukla, and E. Short, ``On textual analysis and machine learning for cyberstalking detection," *Datenbank-Spektrum*, vol. 16, no. 2, pp. 127_135, 2016.