Novel Modelling of the Hash-based Authentication of Data in Dynamic Cloud Environment

Anil Kumar G[1]
Assistant Professor, Department of Computer Science & Engineering, Channabasaveshwara Institute of Technology
Gubbi, Tumkur, India
Visvesvaraya Technological University, Belagavi, Karnataka, India

Shantala C.P[2]
Professor & Head, Department of Computer Science & Engineering, Channabasaveshwara Institute of Technology
Gubbi, Tumkur, India
Visvesvaraya Technological University, Belagavi, Karnataka, India

***Abstract*—A datacenter in a cloud environment houses a massive quantity of data in a distributed manner. However, with the increasing number of threats like data deduplication attack over the cloud environment, it is quite challenging to ascertain data's full-fledged security. In this regard, data integrity and security are highly questionable. A review of existing literature shows that the existing solutions are not much suitable to meet the requirements and support the existing distributed storage system's security demands concerning data integrity due to the usage of the inferior authentication mechanism. Also, the most frequently used public-key encryption is found not to be purely suitable resource constraint devices. Therefore, this manuscript presents a unique model of authentication of data where a simplified hashing proposition has been designed towards scheduling a distributed chain of data. The idea is to perform dynamic authentication that is present of any form of the adversary. The design of proposed scheme is lightweight which offers cross-verifiable hash-based challenges matching scheme with the provision of the non-repudiation of the tractions using the inclusion of a cloud auditor units. The experiment was carried on numerical computing tool considering, data volume, verification count and verification delay as prime performance metrics. The simulation outcomes shows that the proposed system excels in better security performance as well it is flexible compared to the existing system.**

Keywords*—Cloud computing; data deduplication; data integrity; data privacy; data security

I. INTRODUCTION

The collaborative network-based application essentially requires cloud infrastructure to gain various advantages of availability and scalability including data storage requirements. There is various critical application used in the different functional domains of life including healthcare [1], banking [2], automated navigation system [3], transport safety [4], data security [5], secured vehicular network [6], query assessment [7], data authentication [8], selective authentication [9]. In all these applications, compromise of data integrity poses substantial security concerns. If their data are compromised, then a potential economic loss and fatal threats occur on the human being. Therefore, designing an efficient, flexible, robust, and cost-effective data authenticator for verifying integrity is an essential requirement for the data's security. The cloud service usually focuses on building the cloud services' core components, so they outsource the security requirement to the Trusted Third Parties (TTP) [3]. There are pros and cons of relying on the TTP for the data authenticator, and even many of the collusive attacks have taken place in the recent past [10]. Though traditionally there exist many data authenticators, it lacks its feasibility because of few aspects such as the computing system evolving very dynamically. Another factor is that the attackers understand the data-authenticator's working principle and finds a way to break it. Thus, designing a robust and efficient data-authenticator to verify data integrity is an open research problem that requires researchers' attention.

The resource constraint devices fail to verify the integrity by running a local data-authenticator; some of the recent studies recommend blockchain for this purpose. Still, it is at a very nascent stage [11]. In recent times, healthcare systems potentially utilize pervasive computing integrated with the cloud infrastructure, where cloud storage is used to store patient information (P.I.). If these data are exposed to unauthorized users with malicious intension, then the data's integrity gets compromised, and in turn, a wrong diagnosis is performed. Therefore, it is an essential requirement to have a system or a method to verify P.I.'s integrity before utilizing it for medical references. The traditional approach for the verification of data-integrity involves the proprietary stakeholder itself as an authenticator. Another domain of the future system of intelligent transport system aims for a zero tolerance to the accidents that demand higher scalability on message verification operations in lower latency. Therefore, the requirement of data-authenticators adds, also, a low latency based fast data or message authentication. Blockchain technology may be promising to design distributed and strong data authenticator. There are many other applications such as the Internet of Vehicle, Spatial Query in geospatial, big data storage, and data sharing. These exhibit unique challenges and require customized treatment for data authentication for integrity verification. The applications like VANET require low delay-sensitive data authenticator. In contrast, the service-oriented architecture-based application needs to have a data authentication valid for the cross-domain. Another popular application based on the location requires verification of unique queries in low computational complexity. The WSN is used either independently or as a sub-network of IOT; the success of the application solely depends upon the timely delivery of the data using geographical routing protocols, whereas the simple denial of attack brings disruption into the

data delivery process that demands a suitable verifies to isolate the attacker nodes. Apart from these approaches, in the recent past, hardware-level security using FPGA implementation is gaining researchers' attraction, where the IoT devices to the cloud get authenticated at the hardware layer itself. The popularity of content delivery models through the cloud demands a computationally efficient and errorless joint protocol of auditing privacy-preservation and authentication [12]. One another challenge arises in Shared Storage Service (SSS), where it is essential to verify the data integrity effectively in the SSS for data, which is usually performed by the members-based auditing mechanism that poses higher computational overhead. However, the use of the lightweight method ignores security risk [13]. The process of data deduplication and integrity auditing efficacy requires optimal balance to establish a trust and cost factor [14]. The forensic process always requires access to reliable data that might be vulnerable to numerous exploits that. This problem requires a suitable verification system to verify the device's integrity, which fetches the records from the cloud [15]. The third-party-based auditor facilitates the auditing as a service (AaaS) model suffers from many challenges while providing data verification services; such challenges include non-repudiation proof sought by between the auditor and cloud service provider [16]. Integrity verification by cost-effective ways is generally not a very responsible way. The cloud infrastructure is an obvious choice today for the storage as well analytics platform for big data. The service providers make multiple replications to ensure reliable availability of the data. The existing auditing processes lack the security standards, and the overheads and synchronization of the authentication with auditing do not take place simultaneously [18]. The cloud infrastructure is now not only supporting data storage. In contrast, it also provides facilities to operate on it for modification of the data blocks. Still, the traditional remotely operated approach to ensure data integrity lacks the public auditing mechanism, which brings lots of conflicts of interest and credibility [20]. The evolution process will continue as the data verities keep coming into reality and its storage mechanism. This paper proposes a method of authentication of the cloud user over the vulnerable deployment scenario. Simultaneously, the proposed system also implements a mechanism towards auditing the integrity of the cloud data. The paper's organization is as follows: Section II discusses the current work towards data integrity, followed by briefing the research gap and different challenges from the existing system in Section III. Discussion of the proposed method is carried out in Section IV while obtain outcome of the study is briefed in Section V. Finally, Section VI discusses the summary of the proposed paper.

II. Review of Literature

A data-authenticator method for verifying the integrity of the data in the resource constraint context of IoT-based medical record system is proposed in the work of Ding et al. [1]. The model proposes using an edge server as a data authenticator in place of an IoT device, with an objective of cost-effective and independent of the third-party verifier. Blockchain technology is gaining popularity for designing suitable data integrity approaches for the resource constraint devices, as Alotaibi et al. [2] advocated. In the context of the Internet of Vehicles (IoV), only and unique message integrity verification on edge-fog computing layer along with 2-factor authentication is present by Tsaur et al. [3]. The use of the hash chain-PKCS eliminates the use of the certificate that ensures low latency. Spatial query integrity is very sensible for many geospatial applications; a KNN based query message verification method is introduced by Jing et al. [4]. The Hadoop framework for the big data storage (HFBDS) in the cloud does not provide any security support system; Chattaraj et al. [5] proposes a fault-tolerant authentication protocol suitable for HFBDS. Data sharing (D.S.) is quite useful but challenging. Its security is taken care of by ring signature for authenticating data by the data owner itself using certificate and PKI. Still, it suffers bottleneck while scalability that can be overcome by Identity-based ring signature (IBRS). The work of Huang et al. [6], Enhances the IBRS by provisioning forward security to make the system suitable for large scale D.S. In the context of VANET, the message authentication takes place by a joint operation of certificate and signature verification that cause privacy compromise concern. This delay-intensive process problem is studied by (Jiang et al. [7] and proposes an anonymous authentication to completely replace the certificate and signature verification by using the hash code of the message. Still, it limits the conditional security aspect of privacy. The cloud storage is essentially used for storing the spatial GPS data from the location-based applications. Strong authentication provides a vaccine for the possibility of compromising the integrity of the query. The work of Hu et al. [8] proposes a client-side query-result verification authentication model. The model uses a smaller object for the verification, so comparatively less computationally complex computationally, whereas it is not tested for scalability and lacks the auditing. The success of distributed and integrated service-oriented architecture (SOA) is the key mantra of today's web-based service in various domains of function application. Since the information moves out of the original content owner's control that requires a strong verifier for integrity. In this context, a cross-domain verifier is extensively used. Alam et al. [9] describe the cross-domain data authenticator, namely 'xDAuth' that fulfills the integrity and security protocols essentials.To overcome the effect of the denial of attack in geographical routing adopted in WSN, an opportunistic authentication scheme is proposed by Lyu et al. [10], where a cooperative verification process creates a partition between the regular and attacker nodes. An FPGA realization of the verification modules for the data integrity is carried out in Al-Asli et al. [11], which use a re-encryption scheme in a faster way for a huge data file. The content owner hosts their data to the cloud, which is being used by the subscribers. A robust and efficient auditing system requires performing the integrity check by minimizing error. Tian et al. [12] propose third-party management (TPP) light-weighted hash graph auditing method that handles the tradeoff between the security and the computational complexes [13]. Light-weighted secure deduplication for the cloud's data storage provides a balance between encryption and the storage cost by the third-party auditor [14]. The fingerprint of the accessing device and the human attributes are used in designing the verifier for the forensic stakeholder to access the cloud data [15]. To strengthen the third-party auditing system, Liu et al.,

the author in [16] proposed a computationally light-weighted scheme for formal analysis by fine-grain updates of the data. The computational cost for integrity verification is reduced by adopting a new data storing process [17]. Public auditing methods combining the authentication using a hash tree is proposed in the work of Liu et al. [18]. The auditing system for accounting the integrity shall be immune to the impersonation attack; one such work is proposed by Yuan et al. [19]For auditing the shared file integrity in a lower cost. Wang et al. [20] propose data dynamically using a hash tree for the block authentication with strong auditing support to the existing TPA authentication process. A mathematical model of a multi-party agent-based data integrity scheme is proposed by Wang et al. [21] use a multi-copy data process. Sun et al. [22] introduce a hash authentication for big data using the homomorphic scheme; in the work of Lu et al. [23], a remote data integrity scheme is proposed using the homomorphic authenticator with index verification for big data using big graph representation. Zhang et al. [24] proposes a method to balance the cost of storage with lightweight verification. The work carried out by Kavuri et al. [25], Anitha and Nair [26], Kumar & Shafi [27] have also emphasized data security. Apart from this, our prior work [28] [29] and [30] has also studied data integrity.

III. Research Problem

After reviewing all the work of existing data integrity approaches, the following research problems have been identified.

- The existing approaches towards data integrity don't consider the user's role much, which is one significant indicator of vulnerability within any form of network.
- The security is entertained in the form of user authentication and not much on data authentication, making it the server challenging to understand the legitimacy of the data.
- Adopting third parties is more to carry out secure data validation; however, it also affects the data's ownership by the cloud tenants.
- Majority of the existing approaches includes a highly sophisticated set of operation and is quite specific to the form of attack leading to vulnerable data integrity.

Therefore, the problem statement is as follows "Validating the legitimacy of the data over the vulnerable cloud environment and maintaining the highest degree of data ownership is quite challenging." The next section discusses the proposed solution.

IV. Research Methodology

The design of a framework adopts an analytical modeling approach for data integrity to enhance the security level for data privacy. The proposed study's exceptional contribution is to offer a cost-effective solution to authenticate the communicating nodes in a cloud environment. Unlike the existing system, the proposed course emphasizes a more lightweight validation approach with no retention of stale information within the network. Hence, all possibility of any intermediate intrusion is avoided. It is quite challenging to achieve synchronization between data integrity and data deduplication. The cloud storage system achieves an optimal balance between data privacy and storage bottleneck by deduplication. This tradeoff is made feasible using the divide. It conquers rule, so this framework mainly focuses on the auditing aspects of data integrity. Future research direction considers a joint implementation of more robust authentication, data integrity, and data duplication to provide a process protocol for the secure distributed cloud storage system. Therefore, this system model is a sub-framework for offering robust data integrity as a complement contribution to data privacy. The system model consists of three building blocks of the framework that includes: 1) Identity-based Registration and Authentication Block (RAB), 2) Cloud Data-Storage Service Dashboard (CDSSD), and 3) Access Cloud Auditing Management Dashboard (CAMD). This section discusses the modules and their respective design with algorithm implementation towards a research aim elaborately addressing the existing research problem.

A. Identity-based Registration and Authentication Block

The Registration and Authentication Block (RAB) provides access to both the stakeholders, namely, Cloud Tenant (**CT**) and the Cloud Auditor (**CA**). The CT allows two operations = {$\mathbf{ct_R}$, $\mathbf{ct_A}$}, where ct_R is the registration process for the new C.T., and the ct_A is the authentication process for the legitimate C.T. The ct_R takes three attributes to complete the registration process. These attributes are the set ($\mathbf{Sct_R}$) = {$\mathbf{ct_N}$, $\mathbf{ct_E}$, $\mathbf{ct_P}$} which gets updated into the RAB's registration database (auth-RAB). Whereas the ct_A performs authentication of the legitimate C.T. by accepting and matching the value pair of ct_E and ct_P with the corresponding tuple: (ct_E,ct_P) stored in the *auth-RAB-CT*to gain access into the next block of operation of Cloud Data-Storage Service Dashboard (**CDSSD**). A closer look into this module shows that it offers a hierarchy of operations that is beneficial for the inclusion of maximum effort for attackers to have access, which will eventually lead to failure. The process flow of the RAB unit of the framework is shown in Fig. 1.

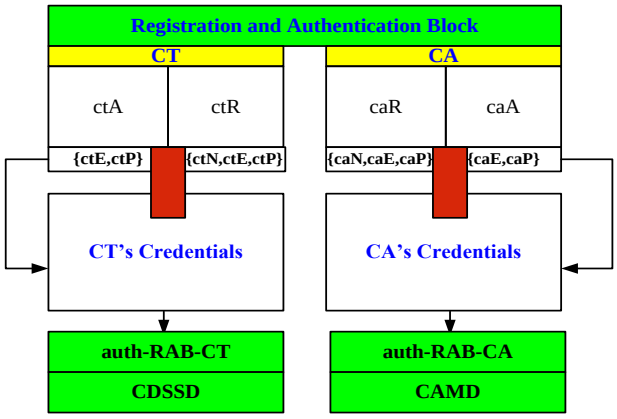

Fig. 1. Process flow of the RAB Block of Framework.

In Fig. 1, the process of registration and authentication of is shown for both cloud tenant and cloud auditor. The registration process takes place considering credential in form of name, email and password, which further gets updated into the identity based registration and authentication database. The

authentication process executes by taking and matching the value pair of credential provided at the time of registration and followed by corresponding tuple set to gain access to the cloud services.

Algorithm 1. Registration and Authentication Block

Input : ct_N, ct_E, ct_P
Output: Auth
Start :
auth-RAB ←$ct_R(ct_N, ct_E, ct_P)$
while Authentication:
if $ct_R(ct_E, ct_P)$ = = auth-RAB(tuple: ct_E, ct_P)
Pass←Auth
Access → CDSSD
else
Suspect Dictionary attack←Access Denied
end
End.

In the same manner, the new C.A. performs registration by providing {ca_N, ca_E, ca_P} credentials to 'ca_R' and while authentication of C.A., by match process of the {ca_E, ca_P} with the *auth-RAB-CA*to gain access cloud auditing management dashboard (CAMD).

B. Cloud Data-Storage Service Dashboard (CDSSD)

This module acts as a bridge of communication between the system and the user. The term dashboard will refer to the user-friendly interface, which the stakeholder uses to store or access their contents over the cloud storage units. Unlike the existing approach, the proposed system offers flexibility to access the user's data and not system-defined, which provides more strength to ownership of data. The CT dashboard, namely: CDSSD, provides a handler to upload the C.T.'s data(ct_D) to the cloud bucket storage (CB_S) in an indexed manner as record-ID(r_{ID}), and every upload of the ct_D maintains a times-stamping instance(ctD-TS) is updated along with the respective ct_D and r_{ID}. The respective C.T. can view their records with the r_{ID}. The simple presentation of the record upload and view is shown in Fig. 2.

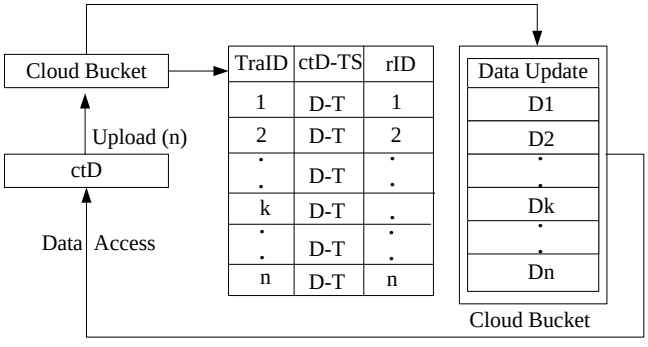

Fig. 2. Cloud Bucket Indexed Data.

The process algorithm is for the Cloud Tenant (**CT**), where the Data Transaction updates carried out to Master Meta-Data Record (MMDT) of c_A is described in Algorithm2.

Algorithm 2. Cloud Tenant (**C.T.**) Data Transaction update to Master Meta-Data Record(**MMDT**) of c_A

Input: ct_E, ct_P, CDSSD
Output:
Start :
∀ *"i"* ct_D∈ *(CT)*$_k$∈{ auth-RAB }
$(Tra_{ID})_i$←$(ct_{Data})_i$
*(*ctD-TS*)*$_i$ ←*f-time(clock)*
MMDT←{Tra_{ID}, ctD-TS, auth-RAB}$_{kth}$
Challenges[cA] ←*RPGF(*cT-P1, cT-P2*)*
Update:
cA[SD]← MMDT ∪ Challenges
End.

The CDSSD provisions a dashboard to all the registeredCloud Tenant. Whenever any registered and authenticated cloud users upload their data, the identity of the cloud tenant and the data records with timestamps gets updated into the Master Meta-Data Record (MMDT) matrix of cA shown in Fig. 3.

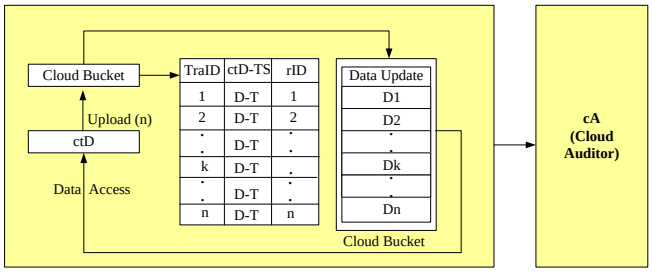

Fig. 3. Kth – cT Data Transaction update to Master Meta-data Record (MMDT) of cA.

To maintain a random seed for the data authentication, two initial seed: {cT-P1, cT-P2} gets generated by the random prime generator function (RPGF), in a very chaotic permutation of randomness, which goes as a challenge to the cA and the complete information of the transaction with the transaction I.D., timestamp and challenges (cT-Ch) gets updates for the commerce of data upload by the respective cTs as seeded data into the cA as cA[S.D].

C. Cloud Auditor Data-Authentication Dashboard (CADAD)

This module is called a cloud auditor, which is meant for performing authentication of the data. This module cross-checks the basic legitimacy of the data. Unlike any existing method, the proposed system harnesses the potential of hashing-based methods to incorporate data security. The novelty of this mechanism is to ensure data integrity and privacy at the same time. The CADAD maintains the updates of the ∀ cT with details of {ctE} and gains access to the number of transactions made by the $(cT)_k$ from cA[S.D.]. For each record, the cA generates a challenge message (**Ch_{msg}**) with the ctD-TS and cT-Ch using an SHA-256 hashing

algorithm. The algorithm for this process is given in Algorithm 3.

Algorithm 3. Data integrity flag using c_A and CPS hashed challenge

Input: ct_E, cA[SD].
Output: DIF
Start:
for ∀ *cA[SD]*, Generate,
Chmsg ←*hash-function (*ct_E, c_A[SD]*)*
Chcsp ←*Hash-fucntion (*ca_E,c_A*[SD])*
end

Data Integrity flag ← [Chmsg ~ Chcsp]
End.

The cA's {Chmsg} and another corresponding challenge message from the CSP as {Chcsp} is used for verifying the proof of authenticity with all the credential matches between thecT, cA, and the CSP with the cT's identity, in-charge auditor, timestamp of data records, data identification number, respective challenges from the cA and the CPS. Based on mutual verification between [Ch_{msg} ~ Ch_{csp}], each data upload gets a Data Integrityflag (DIF) as verified or not verified.

V. Results and Discussions

To perform an assessment, the proposed system constructs a test-bed where there are 50 accesses given for cloud auditors and 100 accesses provided for cloud tenants. The proposed method's implementation is carried out using MATLAB, where the idea is to testify the effectiveness of the proposed algorithm concerning defined performance parameters. The system model maintains and auditing ledgers for non-repudiation. Fig. 4 illustrates the traffic of cloud device access and data authenticator at any time, Δt.

Table I and Fig. 4 above show the traffic count of cloud device access to the data panel either for uploading new data or accessing the uploaded data and delivering the frequency count of access to the security panel of the data authenticator model. From Fig. 4, it can be seen that the analysis is carried out on test sample values of 3 and 6 frequency count of access for cloudlet device and data authenticator showing that data authenticator is capable of validating double the number of the cloud tenants.

Fig. 5 exhibits the analysis of data volume per cloud let devices followed by quantified observation in Table II. The graph trend it can be analyzed that each cloudlet device can hold different volumes of data.

Fig. 6 and Table III exhibits analysis concerning verification count per Data-Authenticator. The analysis from graph trend shows that the data authenticator can validate multiple scores and volumes of data.

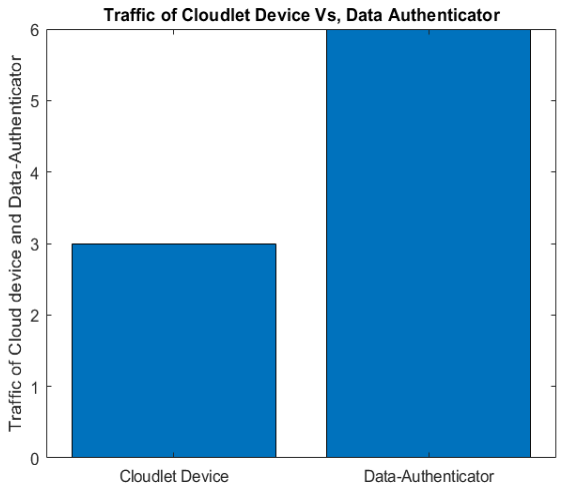

Fig. 4. Analysis of Traffic.

TABLE I. Numerical Outcomes of Access Counts

Traffictype (Stakeholders)	Frequency count of access
Cloudlet Device	3
Data-Authenticator	6

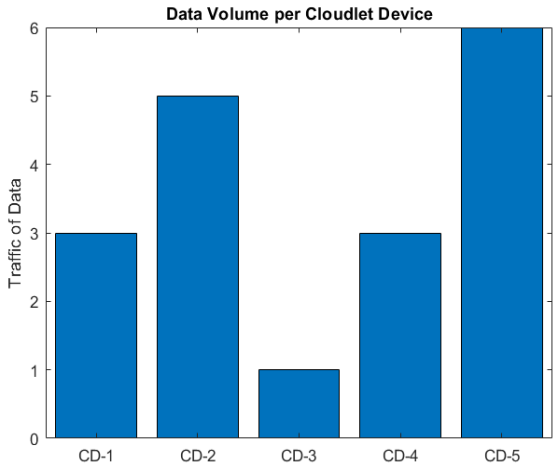

Fig. 5. Analysis of Data Volume.

TABLE II. Numerical Count of Data Volume

Cloud Device	Traffic of Data
CD-1	3
CD-2	5
CD-3	1
CD-4	3
CD-5	6

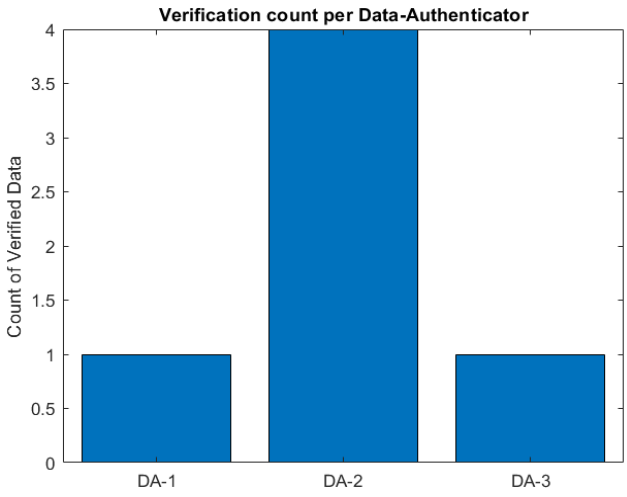

Fig. 6. Analysis of Verification Count.

TABLE III. NUMERICAL OUTCOME OF COUNT OF VERIFIED DATA

Data Authenticator	Count of Verified Data
DA-1	1
DA-2	4
DA-3	1

Fig. 7 highlights that the proposed system offers better performance in contrast to the existing authentication system. Although, with an increase inthe number of entities, the verification delay increases, which is expected, the proposed method exhibits considerably less duration for verification as compared to the existing system. The prime reason behind the proposed system getting better performance is that a simplified hashing-based authentication mechanism is designed which performs a faster assessment without much depending on computational resources dependency or storage demands unlike any existing protocols (shown in Table IV). The conventional technique is associated with complex operation involves a recursive operation in its implementation design and requires large storage space.

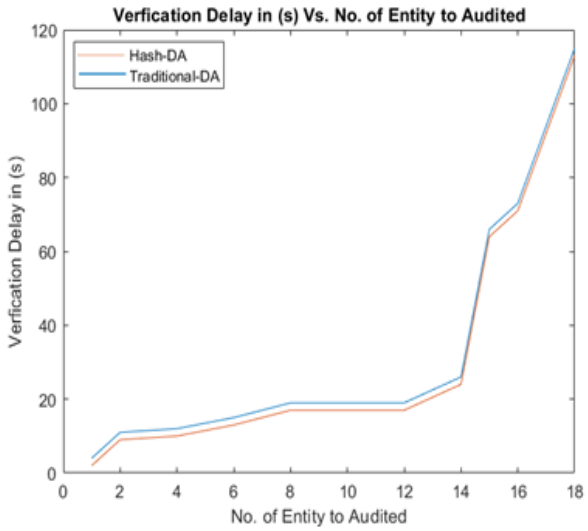

Fig. 7. Analysis of Verification Delay.

TABLE IV. NUMERICAL OUTCOMES OF VERIFICATION DELAY

No of Entity to be Audited	Verification Delay (Hash-DA)	Verification Delay (Traditional-DA)
1	4	2
2	11	9
4	12	10
6	15	13
8	19	17
10	19	17
12	19	17
14	26	24
15	66	64
16	73	71
18	115	113

VI. CONCLUSION

The continuous adaptation of the cloud eco-system for data storage, even for critical applications, raises the robust and efficient data authenticator design for data integrity verification. This paper introduces an analytical framework for a scheme for cross-verifiable hash-based challenges matching scheme for assign a flag of data integrity verified by the data authenticator with the provision of the non-repudiation of the tractions using the inclusion of a cloud auditor units. The performance metric justifies its scalability for the data traffic volume, several devices connected to the cloud for the data upload, and the verification delay lower and consistent. The scheme can be fine-tuned for the adoption in the real cloud scenario for non-repudiated auditing for the data integrity verification by the authenticator. The contribution of this manuscript are: *i*) a simplified hashing-based authentication mechanism is constructed which performs a faster assessment, *ii*) The authentication is performed for both the user as well as data for any target nodes, iii) the proposed system offers almost nil key dependency or storage demands unlike any existing protocols, iv) higher scope of resiliency is incorporated which provides security without having any dependencies of any apriori information of attacker or network. In the future, the system can be extended to synchronize within data confidentiality issues while data deduplication in the cloud storage system. The study intend to adopted lightweight design of encryption technique for data security and hashing mechanism for integrity verification.

REFERENCES

[1] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight Privacy-Preserving Identity-Based Verifiable IoT-Based Health Storage System," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8393-8405, Oct. 2019, doi: 10.1109/JIOT.2019.2917546.

[2] B. Alotaibi, "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review," in *IEEE Sensors Journal*, vol. 19, no. 23, pp. 10953-10971, 1 December 1, 2019. doi: 10.1109/JSEN.2019.2935035.

[3] W. Tsaur and L. Yeh, "DANS: A Secure and Efficient Driver-Abnormal Notification Scheme with IoT Devices Over IoV," in *IEEE Systems Journal*, vol. 13, no. 2, pp. 1628-1639, June 2019.

[4] D. Chattaraj, M. Sarma, A. K. Das, N. Kumar, J. J. P. C. Rodrigues and Y. Park, "HEAP: An Efficient and Fault-Tolerant Authentication and

Key Exchange Protocol for Hadoop-Assisted Big Data Platform," in *IEEE Access*, vol. 6, pp. 75342-75382, 2018.

[5] X. Huang et al., "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," in IEEE Transactions on Computers, vol. 64, no. 4, pp. 971-983, 1 April 2015. doi: 10.1109/TC.2014.2315619.

[6] S. Jiang, X. Zhu and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193-2204, Aug. 2016.doi: 10.1109/TITS.2016.2517603.

[7] L. Hu, W. Ku, S. Bakiras and C. Shahabi, "Spatial Query Integrity with Voronoi Neighbors," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 4, pp. 863-876, April 2013. doi: 0.1109/TKDE.2011.267.

[8] Q. Alam et al., "Formal Verification of the xDAuth Protocol," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1956-1969, Sept. 2016. doi: 10.1109/TIFS.2016.2561909.

[9] C. Lyu, X. Zhang, Z. Liu, and C. Chi, "Selective Authentication Based Geographic Opportunistic Routing in Wireless Sensor Networks for Internet of Things Against DoS Attacks," in IEEE Access, vol. 7, pp. 31068-31082, 2019.doi: 10.1109/ACCESS.2019.2902843.

[10] Y. Jing, L. Hu, W. Ku, and C. Shahabi, "Authentication of k Nearest Neighbor Query on Road Networks," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 6, pp. 1494-1506, June 2014. doi: 10.1109/TKDE.2013.174.

[11] M. Al-Asli, M. E. S. Elrabaa, and M. Abu-Amara, "FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for cloud-integrated Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 446-457, Feb. 2019.doi: 10.1109/JIOT.2018.2864513.

[12] B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," in IEEE Access, vol. 4, pp. 7899-7911, 2016. doi: 10.1109/ACCESS.2016.2621005.

[13] J. Tian and X. Jing, "A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage," in IEEE Access, vol. 7, pp. 68071-68082, 2019. doi: 10.1109/ACCESS.2019.2916889.

[14] J. Wu, Y. Li, T. Wang, and Y. Ding, "CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing," in IEEE Access, vol. 7, pp. 160482-160497, 2019. doi: 10.1109/ACCESS.2019.2950750.

[15] A. Liu, H. Fu, Y. Hong, J. Liu, and Y. Li, "$LiveForen$: Ensuring Live Forensic Integrity in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, pp. 2749-2764, Oct. 2019. doi: 10.1109/TIFS.2019.2898841.

[16] C. Liu et al., "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2234-2244, Sept. 2014.doi: 10.1109/TPDS.2013.191.

[17] J. Li, X. Tan, X. Chen, D. S. Wong, and F. Xhafa, "OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices," in IEEE Transactions on Cloud Computing, vol. 3, no. 2, pp. 195-205, 1 April-June 2015.doi: 10.1109/TCC.2014.2366148.

[18] C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, "MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud," in IEEE Transactions on Computers, vol. 64, no. 9, pp. 2609-2622, 1 September 2015. doi: 10.1109/TC.2014.2375190.

[19] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1717-1726, Aug. 2015. doi:10.1109/TIFS.2015.2423264.

[20] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.doi: 10.1109/TPDS.2010.183.

[21] C. Wang and X. Di, "Research on Integrity Check Method of Cloud Storage Multi-Copy Data Based on Multi-Agent," in IEEE Access, vol. 8, pp. 17170-17178, 2020. doi: 0.1109/ACCESS.2020.2966803.

[22] Y. Sun, Q. Liu, X. Chen and X. Du, "An Adaptive Authenticated Data Structure With Privacy-Preserving for Big Data Stream in Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3295-3310, 2020.doi: 10.1109/TIFS.2020.2986879.

[23] Y. Lu and F. Hu, "Secure Dynamic Big Graph Data: Scalable, Low-Cost Remote Data Integrity Checking," in IEEE Access, vol. 7, pp. 12888-12900, 2019.doi: 10.1109/ACCESS.2019.2892442.

[24] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676-688, March 2017. oi: 10.1109/TIFS.2016.2631951.

[25] Satheesh K S V A Kavuri, Gangadhara Rao Kancherla, BasaveswararaoBobba, "An Improved Integrated Hash and Attributed based Encryption Model on High Dimensional Data in Cloud Environment," International Journal of Electrical and Computer Engineering, Vol.7, No.2, 2017.

[26] Anitha K L, T.R. Gopalakrishnan Nair, "Data storage lock algorithm with cryptographic techniques," International Journal of Electrical and Computer Engineering, Vol.9, No.5, 2019.

[27] Y. Kiran Kumar, R. Mahammad Shafi, "An efficient and secure data storage in cloud computing using modified RSA public-key cryptosystem," International Journal of Electrical and Computer Engineering, Vol.10, No.1, 2020.

[28] Anil Kumar G and A.S.Poornima, "A Survey on Data Integrity Methods in Cloud Storage," EJERS, European Journal of Engineering Research and Science, Vol. 1, No. 5, November 2016.

[29] Anil Kumar G., Shantala C. P.,"An extensive research survey on data integrity and deduplication towards privacy in cloud storage," International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 2, April 2020, pp. 2007~2018.

[30] Anil Kumar G., Shantala C. P.," Framework towards Higher Data Privacy by Novel Data Integrity Scheme," 1st International Conference on Innovation in Computer Science, Electrical and Electronics Engineering (ICICEE), 2020.

AUTHORS' PROFILE

Mr. Anil Kumar G is a Research Scholar in the Computer Science and Enginee ring department of Channabasaveshwara Institute of Technology at Visvesvarahya Technological University. He perused his bachelor's degree in Computer Science & Engineering from Gulbarga University, Karnataka, India, and masters in Computer Science & Engineering from Dr. MGR Educational Research Institute, Chennai, India. Mr. Anil Kumar has good academic and research experience in Computer Networks, Unix Systems Programming, Cloud Computing with many publications.

Dr. Shantala C P is Professor & HOD in the Computer Science and Engineering department of Channabasaveshwara Institute of Technology at Visvesvaraya Technological University. She is vice-principal of Ch annabasaveshwara Institute of Technology. She has completed her Ph.D. in the area of Data Security and Masters in Computer Science & Engineering. Her research interests lie in Network & Data Security, Cloud Storage, Data Mining & Brain-Computer Interface. Her research works brought her various awards like Seed Money for Young Scientist from VGST & Women Achiever Award from IEEE.