International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient Secure and Privacy Cloud Auditing in Winternitz Signature Scheme

M. Mageshwari[1], R. Naresh[2]*

Submitted: 18/10/2023 **Revised:** 10/12/2023 **Accepted:** 14/12/2023

Abstract: This cloud computing approach gives customers access to many platforms and delivers scalable, on-demand services whenever and wherever they are needed. The main issues in an outsourcing approach occur because users no longer possess access and ownership of their data, which means it is more challenging to conduct appropriate security audits. Winternitz Signature Scheme (WSS) is an extremely important cryptosystem. Not only may many signatures be compressed into a shorter signatures, but also guarantee the authenticity of each signature taking part in the combination by checking if the resultant aggregate signature is valid. Cloud server, Third Party Audit (TPA), and Data owners providers are all needed to complete the service. For the data owner, these processes include dividing the blocks in file, each encrypts of them, calculating a hash key, then merging them back together to produce a signature, and finally transmitting the result. The new audit method has used to cope with all these requirements. In this approach, the cloud server maintains a verifiable secure signature scheme, allowing for batch auditing. When it comes to practical arrangements, the efficiency and security of our approach are shown by the fact that it is reducing the computing and communication auditing process cost, which is particularly beneficial.

Keywords: *Cloud Server, Security Audits, Third party Audit (TPA), Signature scheme*

1. Introduction

Transmission of data and exchange has dramatically grown due to the advancement in the speed of communication and networking in recent times. At the same time, there is increasing demand for digital media, including videos, images, and music. As a result, businesses and individuals alike have spent an excessive amount of money on providing IT services. (Tian et al., 2019) [2]. Traditional storage methods are unlike cloud storage. This allows users to store more data at the same place, as well as access the data from different geographical areas. Users may utilize any device linked to the networks and linked to the public cloud to access data sources from anywhere and at any time (Sun et al., 2020) [4]. Even while cloud storage has many advantages, it comes with its security concerns and even assaults. In the first instance, data stored in the cloud may be compromised by hackers or even wholly deleted, thereby compromising confidentiality, integrity, and availability. In addition, outsourced data is vulnerable to both illegal activities by cloud providers (CSPs) and the malicious actions of insider threat actors (ITAs) (M et al., 2018) [6].

Securing cloud services is essential since the service provider gives customers and users complete security. This article examines the challenge of verifying public integrity in dynamic data when people utilize group revocation. These are the main contributions:

- ✓ We provide a multi-user auditing method on cipher-text databases for secure and efficient shared information integration.
- ✓ Group commitment, asymmetrical group key agreement, and group signature are used to create a more effective data auditing system.

Cloud computing uses data auditing to data storage is protected. It is possible for a user (the data's owner) to conduct auditing themselves, or for a third-party auditing company to do so on their behalf, to validate user data [1]. Data saved in the cloud should be protected so that the integrity of the information is not compromised. Data broke down the verified role into two groups: user-only audit, wherein the user or the entity that has saved the data may attest to the data's integrity. The server is the only one who may challenge the data [3].

[1]*Research Scholar,*
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Kattankulathur,
Chengalpattu, Chennai, Tamilnadu, India-603 203.
Email: mm6344@srmist.edu.in
[2*]*Associate Professor,*
Department of Networking and Communications,
SRM Institute of Science and Technology, Kattankulathur,
Chengalpattu, Chennai, Tamilnadu, India-603 203.
Email: nareshr@srmist.edu.in

2. Related Works

Private auditing systems enable auditing exclusively by the data owner, whereas public auditing schemes allow anybody to audit audits. With cloud computing, personal audit schemes are appropriate for businesses with sensitive information [5]. As with internal auditing, however, public auditing is gaining popularity for companies that need large amounts of data backup and have limited computational resources. The data-sharing system suggested by (Lu et al., 2020) [8] offered private auditing. Auditing may do all security checks before the data is made available to consumers. In addition, they created a method in which data owners may now operate both their device and the devices of the data requesters [7].

A method using anonymity to handle confidentiality problems related to cloud computing was developed by (Wang et al., 2009) [10]. This cloud-based solution hides part of the data from users while processing and uploads it to the cloud [9]. The cloud provider finds this data, combines it with the knowledge it already has, and then utilizes this anonymous data to get the intended result. With conventional cryptography, key management required. Thus, it is a productive and easy process. Applying this strategy will not be an appropriate choice for all providers [11].

According to the researchers' (Daniel et al., 2019) [12], a lightweight reduction and audit protocol using to find the damaged data block by cuckoo filter. The added delay and storage requirements do result in additional computational latency and storage requirements [13]. Finally, large-scale distribution systems that possess sophisticated computing capability are essential. A safe and privacy-preserving method for critical management systems suggested by (Wang et al., 2019) [14] identifies identities throughout the auditing process. To better enable data dynamics, authentication, continued their research. This authentication technique applied to every data block. Nevertheless, it has significant security issues relating to respond attacks, among other things [15].

Verification time rises as a result. Public audit, in which anybody, not the client, may question the server provided by TPA, is the second core benefit of the web application server. TPA is a kind of organisation that used to serve the needs of the customer .This package provides everything essential to do an integrity verification job, and it also helps decrease the client's overall costs. A condition of reasonable data security is that TPA needs to audit cloud data storage but does not require the user first to download the local copy of data. Additional online load for cloud users should not be imposed (Cong et al., 2009) [16].

The specific solution to the distributed storage problem is a portion of this article, in which both discussion and application provided. The first option is a perfectly innocent solution. This solution, however, cannot, in general, handle this problem [17]. The second approach offers a slight improvement but has a considerable extra cost, which is impractical when combined in real-world situations. As a result of the central convention that follows, the efficiency of the two fundamental arrangements increased substantially (Priyadharshni et al., 2015) [18].

However, the TPA reveals the identities of its users when conducting audits. As previously stated, a new technique, known as secret key verified based tags, was put forward to limit this. In contrast, (Liu et al., 2014) [20] suggested a new approach that used an MHT database structure and an additional layer of security that used multiple copies [19]. This approach ensures consistent, real-time updates to dynamic data and effective, ongoing validation for many instances concurrently. However, this has a storage overhead issue since many copies need storage. (Chen et al., 2016) [21] Introduced another CLAS method, but was susceptible to public major replacement aggression and honest but inquisitive KGC assaults but (Li et al.2018) [22] showed that it was still safe in the midst of malevolent, but passive KGC attacks.

3. Proposed Method

This section outlines the system cloud storage concept in great depth. This article examined the public integrity auditing design issue, focusing on including group user revocation in shared dynamic data sets. According to this study, the data auditing paradigm in cloud computing and came up with an auditing protocol, which is far simpler than their previously stated O(n) audit complexity (log n). Figure 1and 2 shows the proposed method architecture and flow chart to reduce complexity.

User - holds which has enough amounts of data files for outsourcing and which may at a later point apply modifications, deletions, insertions, or appends to that data. Dependents (the entity itself, or one of its parts) are wholly reliant on a cloud service provider for data upkeep. A common descriptor of entities is that their limited resources define them.

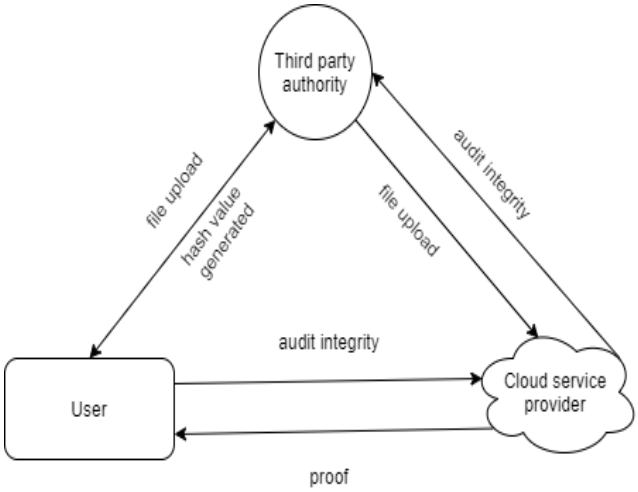

Fig. 1. Proposed System Design

Cloud service provider - An entity with all of the resources it needs, such as computing power and available storage space, has no limits on the number of resources it may use. The task is to ensure the outsourced data is safe and secure. an untrusted entity in CSP terms is known as an "untrusted CSP."

Third party authority - TPA is a capable data auditor for records and lowers the computational burden of auditing user data. It is an entity with complete confidence from both the CSP and the user.

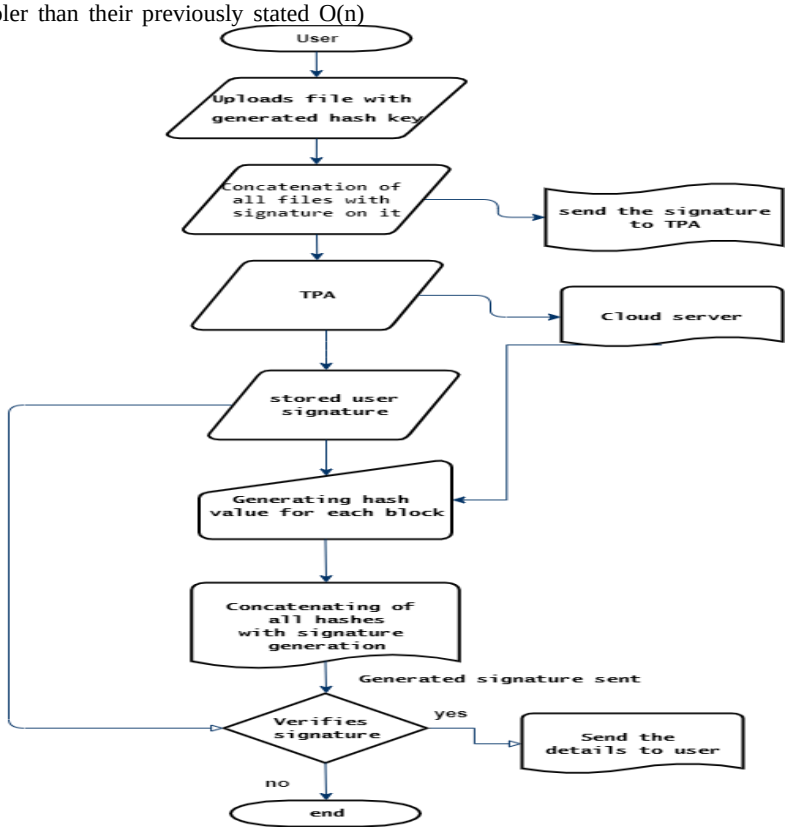

Fig. 2. Flow Chart Design

4. Winternitz Signature algorithm(WSA)

M = {0, 1} k , 2 ∗ k needs to be stored in order to sign a message M = {0, 1} k. A hash function must contain at least 160 bits to be secure. So, for the private and public keys to be at least 320 bits, the private key has to have at least 320 × 2 × k = 640 × k bits. Because most messages hashed before being signed, a message of size 160 bits, M, will almost always have a hash size of k. It is possible to decrease the signature size at the expense of a certain number of hash operations while under the Winternitz One-Time Signature Scheme (WOTS). Figure 3 shows the Building the values bi and the checksum C.

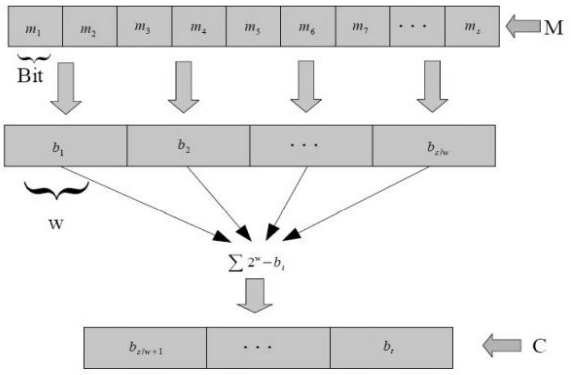

Fig. 3. Constructing bi values and Checksum C

4.1 Key Generation

This cryptography hash function maps values in the range of 0 and 1 to values in the range of 0 and 1. When using the w-parameter with w ∈ N, the initial value is w, and the subsequent value is

$$t = \lceil {}^{S}/_{W} \rceil + \lceil (\lfloor \log_2 \lceil {}^{S}/_{W} \rceil \rfloor + 1 + w)/w \rceil$$

Random numbers of t is $X_1, \ldots X_t \in \{0,1\}^x$

To decrease the number of parameters, the size of the signature must rise. Now we're going to choose random numbers X1, X2, X3, and Xt, which are all $\{0, 1\}^s$. The private key is X = ($X_1 \parallel \ldots \parallel X_t$). After generating $Y_i = H^{2w-1}(X_i)$ for i = 1, 2, 3……t , the public key Y produced. Figure 4 shows the Signature generation and verification with the Winternitz One-Time Signature Scheme.

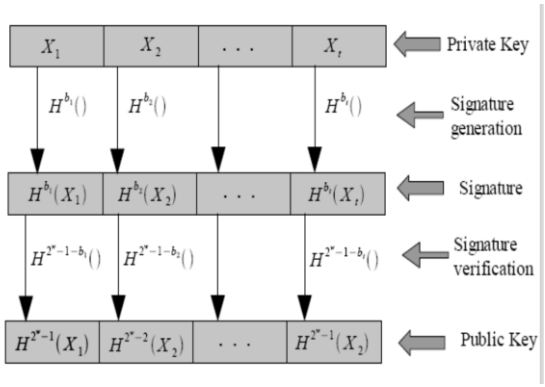

Fig. 4. Winternitz One-Time Signature Scheme for Signature Creation and Verification

4.2 Generating Signature

Earlier making an assumption, consider this idea: Let M = m1, m2, and so on be simply the text to be verified, and X_1, X_2, and so on be the private key. Finally, w and t have already mentioned before. The message M made up of ⌈s/w blocks of length w⌉ blocks, each one labeled s or w. If a message is required, the data is prefilled with zeros from the left first. Because of this, we now consider bi as being encoded as a particular block's integer and calculate the checksum.

$$C = \sum_{i=1}^{\lceil x/y \rceil} 2^w - b_i$$

Finally, we created blocks of $\lceil (\lfloor \log_2 \lceil {}^{S}/_{W} \rceil \rfloor + 1 + w)/w \rceil$ with the length of w. C is padded with 0s from the left, if required. Currently, we represent the integer value of the block bi as the bi integer and then calculate sigi = H^{bi} (X_i) for I = 1, 2, 3, etc. using H_0 (X_i) = X_i. In general, the signature sig = (sig_1||...||sig_t) of the message M is the concatenation of all signatures, with sig_1 as the first element, and so on, until the last signature (sig_t).

4.3 Verification of Signature

For signature verification sig = (sig_1||…….||sig_t) for given message M = $\{0, 1\}^s$

So computing parameters are b_1…. b_t same as generation of signature.

$$sig'_i = H^{2^w - 1 - b_i}(sig_i) = H^{2^w - 1 - b_i}\left(H^{b_i}(X_i)\right) = H^{2^w - 1}(X_i) = Y_i$$

hence $Y' = H(sig'_1||\ldots\ldots sig'_t)$ equals Y = H(Y1||...||Yt) the signature is valid. Otherwise the signature is refused.

4.4 Parameter Choosing

It is a versatile system since it allows the use of many different values for the parameter w. A trade-off between the size of the signature and the time it takes to calculate w may accomplish it using this parameter. Selecting a larger parameter w will lead to a lower signature size. Still, it will also increase the required time to generate and verify signature. Using the variable w, we'll now look at the signature size.

Recommended signature size: A signature is (sig_1|...|sig_t) where each block consists of exactly t sig_i. For each block, the hash output length is equal to the length of one hash output. The signature size is the signature size is proportional to the parameter w by way of the inverse relationship.

Key generation time: For generating keys, random numbers Xi must be selected, and the base 2 logarithm of (Xi) must be calculated for about t seconds. As a result,

gen_{time} = 2w - 1 S / W ∗ $hash_{time}$ + $rand_{time}$ = O(2w) S / W ∗ $hash_{time}$ + O(1/w) $rand_{time}$.

In other words, as the amount of w rises, the time it takes to generate keys grows exponentially.

Sign time (sig_{time}): To create the signature, calculate sigi (as many times as needed). Average hash operations must be done, since this SIG_I (X_i) is being generated with

average (wP−1j=12j)/w =2w−2w.

signing cost of s/w = s/w × (2w − 2)/w (2w).

Verification time (ver_{time}): To verify a message signature, it must be calculated approximately equal to the number of seconds or window of time. The approximation for one sig_i = $H^{2w-1-bi}$ is calculated as: b_i <= 2^w − 1 / w.

Average = $\left(\sum_{j=1}^{w-1} 2^j\right)/w = \frac{2^w - 2}{w}$

In general, above equation represents the number of hash operations. Signature verification and verification time are the same:

ver_{time}=sig_{time}≈s∗(2^w−2)/w^2∗$hash_{time}$ = O(2^w).

Therefore, the optimum value of parameter w relies on the resources available. If the signing is quick enough, the signature size may reduced by increasing w. However, the signature time grows exponentially, the signature size drops linearly, thus it is not advised to use too large a number for w.

5. Result and Discussion

The result from the network performance following table indicates that the key is needed to generate a signature with verification key. The time needed to encrypt and decode the data called computational time. An algorithm efficiency determined by the short calculation time. Figure 5 illustrates the time variation for both the proposed and current WSA methods. For WSA, the calculation time is 30 ms and for the symmetric cypher block suggested is 7, 5 ms. The optimum reduction in the task suggested provides a computer time savings of 75%.

Table 1. Individual signature generation cost

S.NO	Time(ms)	Key
1	120	5
2	250	8
3	350	10
4	400	18

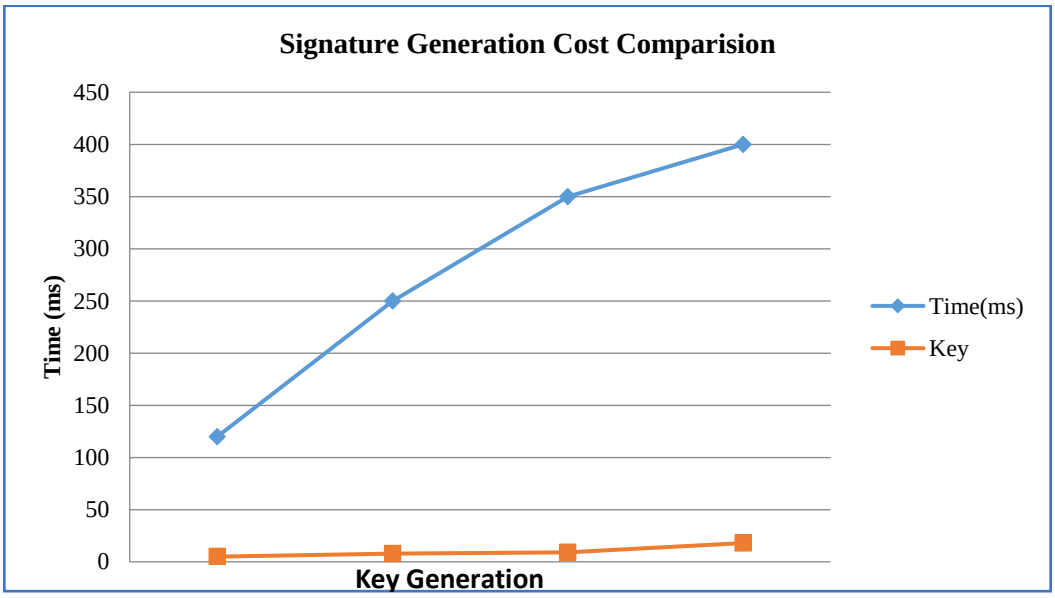

Fig. 5. Signature generation cost comparison

6. Conclusion and Future work

It recommended that a secure and robust privacy mechanism implemented to protect public audits. Using a TPA (Third Party Auditor), which audits without choosing a copy of the data, it is possible to preserve cloud privacy while still doing public auditing. The data was partitioned into parts and then stored in encrypted forms in the cloud storage to keep the data secret. On request of the customer the data integrity is checked by TPA by checking both signatures. It simply checks whether or not the saved data are manipulated and notifies the user. An effort made to overcome the constraints of the current audit system. All of the system's components must implement to establish a successful audit scheme. Future data operations such as updating, removing, and adding data will be performed on dynamic data.

References

[1] A. Saranya, R. Naresh "Cloud Based Efficient Authentication for Mobile Payments using Key Distribution Method", Journal of Ambient Intelligence and Humanized Computing, Springer, 02 January, 2021. DOI: 10.1007/s12652-020-02765-7

[2] H. Tian, F. Nan, H. Jiang, C.C. Chang, J. Ning, Y. Huang "Public auditing for shared cloud data with efficient and secure group management", Inf. Sci., 472 (2019), pp. 107-125.

[3] R. Naresh, P. Vijayakumar, L. Jegatha Deborah, R. Sivakumar, "A Novel Trust Model for Secure Group Communication in Distributed Computing", Special Issue for Security and Privacy in Cloud Computing, Journal of Organizational and End User Computing, IGI Global, Vol.32, No. 3, September 2020, Pp. 1-14. DOI: 10.4018/JOEUC.2020070101

[4] Y. Sun, Q. Liu, X. Chen, X. Du "An adaptive authenticated data structure with privacy-preserving for big data stream in cloud" IEEE Trans. Inf. Forensics Secur., 15 (2020), pp. 3295-3310.

[5] A. Saranya, R. Naresh "Efficient mobile security for E health care application in cloud for secure payment using key distribution", Neural Processing Letters, Springer, 2021, DOI: 10.1007/s11063-021-10482-1

[6] He M, "Certificateless provable data possession scheme for cloud-based smart grid data management systems", IEEE Trans. Ind. Inf., 14 (3) (2018), pp. 1232-1241.

[7] R. Naresh, M. Sayeekumar, G. M. Karthick, P. Supraja, "Attribute-based hierarchical file encryption for efficient retrieval of files by DV index tree from cloud using crossover genetic algorithm", Soft Computing, Springer, Vol.23, No. 8, 2019, Pp. 2561-2574. Doi: https://doi.org/10.1007/s00500-019-03790-1

[8] X. Lu, Z. Pan, H. Xian "An efficient and secure data sharing scheme for mobile devices in cloud computing" J. Cloud Computing., 9 (1) (2020), pp. 1-13.

[9] P. Vijayakumar, R. Naresh, L. Jegatha Deborah, SK Hafizul Islam, "An efficient group key agreement protocol for secure P2P communication", Security and Communication Networks, Wiley, Vol.9, No.17, pp.3952–3965, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/abstract

[10] Wang J, Zhao Y et al., "Providing Privacy Preserving. In cloud computing", International Conference on Test and Measurement, vol. 2, pp. 213–216, 2009.

[11] P. Vijayakumar, R. Naresh, SK Hafizul Islam, L. Jegatha Deborah "An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies", Security and Communication Networks, Wiley, Vol.9, No.18, pp.5085–5097, 2016. http://onlinelibrary.wiley.com/doi/10.1002/sec.1578/full

[12] Daniel, E., Vasanthi, N.A: LDAP: a lightweight deduplication and auditing protocol for secure data storage in cloud environment. Clust. Comput. 22(1), 1247–1258 (2019)

[13] R. Naresh, M Meenakshi, G Niranjana, "Efficient study of Smart Garbage Collection for Ecofriendly Environment", Journal of Green Engineering, Vol.10, No.1, pp.1-10, Feb 2020.

[14] Wang, T, An alternative approach to public cloud data auditing supporting data dynamics. Soft Computing. 23(13), 4939–4953 (2019).

[15] R Divya Mounika, R. Naresh, "The concept of Privacy and Standardization of Microservice Architectures in cloud computing", *European Journal of Molecular & Clinical Medicine*, Vol 7, No 2, Pages 5349-5370, Dec 2020.

[16] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. http://eprint.iacr.org/2009/579.pdf
[17] R. Naresh, AyonGupta, Sanghamitra, "MALICIOUS URL DETECTION SYSTEM USING COMBINED SVM AND LOGISTIC REGRESSION MODEL", International Journal of Advanced Research in Engineering and Technology (IJARET), Vol.10, No.4, pp. 63-73, May 2020.
[18] Priyadharshni, Geo Jenefer. G "Enhancing Data Security in Cloud Storage Auditing With Key Abstraction" Vo.2, Issue 2, Oct 2015.
[19] M. Meenakshi, R Naresh, S Pradeep "Smart Home: Security and Acuteness in Automation of IOT Sensors", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. 9, No. 1, pp. 3271- 3274, Nov 2019.
[20] Liu, C., et al.: MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud. IEEE Trans. Comput. 64(9), 2609–2622 (2014).
[21] Chen Y C, Tso R, Mambo M, Huang K, Horng G (2015) Certificateless aggregate signature with efficient verification. Security and Communication Networks8(13):2232–2243
[22] Li J, Yuan H, Zhang Y (2018) Cryptanalysis and improvement for certificateless aggregate signature. Fundamental Informatica
[23] Mageshwari. M and Dr.R.Naresh," Survey on Cloud Auditing by using Integrity Checking Algorithm and Key Validation Mechanism", *Proceedings of International Conference for information and communication Technology'-(ICTCS- 2022).* Lecture Notes in Networks and Systems (LNNS, volume 396) DOI: 978-981-16-9967-2, 2022.
[24] Mageshwari. M and R. Naresh," Decentralized Data Privacy Protection and Cloud Auditing Security Management", *Proceedings of International Conference on Computing, Communication, and Intelligent Systems-(ICCCIS-2022).* DOI:10.1109/ICCCIS56430.2022.10037676, 2023.
[25] S. Sakthipriya, R. Naresh, Effective Energy Estimation Technique to Classify the Nitrogen and Temperature for Crop Yield Based Green House Application, Sustain. Comput. Inform. Syst.35 (2022).
[26] K. L. Narayanan and R. Naresh, "Improved Security for Cloud Storage Using Elgamal Algorithms Authentication Key Validation," 2023 International Conference for Advancement in Technology (ICONAT), Jan. 2023, doi: 10.1109/iconat57137.2023.10080619, 2023.