Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan *Vol. 28 No. 1-2023*
ISSN:1813-1786 (Print) 2313-7770 (Online)

Multi-Layer Token Framework for Data Protection in Cloud Computing

A. Sheikh[1], S. S. Bhatti[2], M. Abrar[3]

[1]*Department of Computer Science, National College of Business Administration and Economics, Multan, Pakistan*
[2]*Department of Information Sciences, Division of Science & Technology, University of Education Lahore, Pakistan*
[3]*Department of Electrical Engineering, Bahauddin Zakariya University Multan, Pakistan*

[3]mabrar@bzu.edu.pk

Abstract- Today, no one can deny the tremendous effects of cloud computing as it provides access to lot of computing resources including infrastructure, hardware, network, server and applications services to its users. These services are controlled by third party known as Cloud Service Providers. Despite the flexibility and scalability of the cloud computing which has given the business a colossal revolution, privacy is still a major issue which cannot be abolished or ignored. With the development of cloud computing, privacy security issues have become increasingly prominent, which is of concern to industry and academia. Our research progress review the privacy, security and data storage issues of cloud computing. Firstly, we discuss some privacy, security and data storage issues; and then advise an inclusive privacy protection framework by implementing numerous data protection technologies. Secondly, we elaborated the research evolution of some technologies, alike data encryption technique, key and token generation policies at authorization layer, acknowledgement of data at privacy layer and access control and generation of transaction codes at verification layer. Thirdly, we proposed a token generation algorithm. Lastly, we discuss the parameters include in the proposed technique, comparison of token generation base on different attributes, features and strengths and concluded with the possible future research directions. Moreover, PHP language is used for API and RDMS (MySQL) is used as database tool for software development and testing process. Android Studio and Ionic framework was used for frontend development.

Keywords- Cloud Computing, Authorization, security, privacy, Data sensitivity, Multi-layer token framework

I. INTRODUCTION

Cloud Computing allows centralized storage of data which can be access anywhere, anytime with the means of any telecommunication device. We are availing enormous services like email, file sharing and storing, data backups, live streaming, e-learning through simulation and virtual classrooms, social media, e-commerce and many more because of which we cannot deny the importance of Cloud Computing [1]. Today we have enormous organizations which are offering free Data storage on Cloud to a specific limit including Windows Azure, Google Drive, OneDrive, Dropbox, Amazon Drive, Symantec, MEGA, pCloud, MediaFire, Box, FlipDrive, HiDrive and others. These organizations provide free service to an extinct and then user has to purchase its services if user's storage exceeds the free usage limit. Cloud computing basically refers to the Big Data. They are always hands in hands. Cloud Computing has emerged a new trend in business. Cloud Computing has opened a new gate by re-arranging pool of resources [2] and providing the user their on demand services [3]. Data Management through Cloud Computing has revolutionized the Information Technology (IT) industry. Just because of its rapid growth and scalability; a small business can even be established with in an office of two rooms now a days and one of its major reason is Cloud Computing. Small and medium companies acquiring the facility of Cloud are facilitated by the best software and a number of fast services. However, dealing with such a large amount of Data is a challenge itself because data is increasing rapidly and data can be static and dynamic which includes social media data, digital libraries data, physical data [4], healthcare data, dynamic sensor data [5] and others.

In spite of; the unbeatable effects of Cloud Computing over both small and large scale businesses the problem is when organizations focus

on a cloud system, they are most concerned about the data privacy. As the data over cloud is coming from shared pool of resources which is managed through servers and is retrieved through Internet [6] and there is: Firstly, always a chance of leakage or theft of data. Secondly, if the clients want to move from one Client Service Provider (CSP) to another there may be a chance of data leakage or any of the cloud administrator may also take a glance of data kept over the cloud network. Thirdly, data which is being accessed by any user has the authority to access it or not.

Several authors have proposed various techniques of data secrecy, data privacy, reliability, and availability of data by implementing encryption techniques, implantation of identity and access controls, data backup techniques etc.

The proposed system deals with this issue where, working in a shared pool of resources, the data of any specified organization or end user is not accessible by any other organization or end user, moreover it is even not accessible by the administration itself. Protection and sensitivity of private data, the privacy of data, implementation of the proposed framework and its architecture verification is the basic concern of this paper.

The sections of paper concludes literature review, proposed framework, algorithms over different layers, proposed token generation algorithm, parameters of proposed technique, result discussion, features and strengths of proposed technique and conclusion.

II. Literature Review

Cloud Computing is developed on the base of a model of on-demand, self-service of network access having a pool of resources. According to United States National Institute of Standards and Technology (NIST) Cloud Computing is a source of "for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal effort" [7]. NIST also elaborates that a Cloud Service providing company should also commit these five characteristics: resource pooling, on-demand self-service, rapid elasticity [8], worldwide network access and measured service [9].

A. Services in Cloud Computing

With respect to these resources Cloud Computing is distributed in three types of service named as IAAS (Infrastructure as a service), PAAS (Platform as a service) and SAAS (Software as a service) [10].

I. Infrastructure As a Service

IAAS only provides the facility of Infrastructure which includes the virtual machines of cloud computing and virtual storage [11]. Amazon web services and Rackspace cloud are most common examples of IAAS providers.

II. Platform As a Service

PAAS (Platform as a Service) provides the facility of both Infrastructure and Platform which includes the virtual machines, it applications development and their deployment tools. Some famous PAAS providing vendors are Windows Azure, Google App Engine, Amazon's Relational Database Service (RDS) [12] and force.com etc.

III. Software As a Service

In SAAS (Software as a Service); software services are provided to end users [13]. Some famous SAAS providing companies are Google Apps, salesforce, dropbox and others. Some of the enormous features and benefits of Cloud Computing are shown in Fig.1.

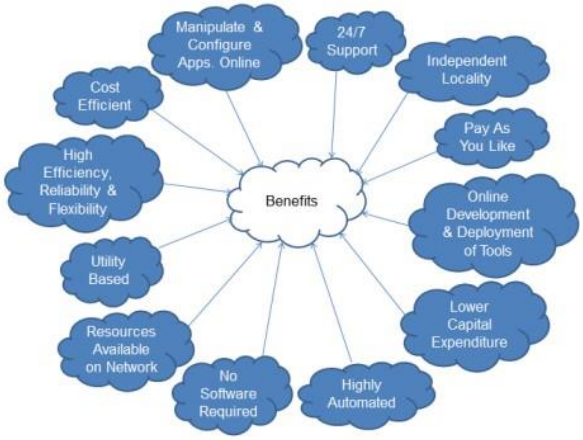

Fig. 1: Benefits of Cloud computing

B. Deployment of Cloud Computing

Moreover, the deployment of cloud is characterized as Public, Private, Hybrid and Community.

i. Public Cloud

Public cloud allows the services to be accessible by general public but a limited number of people [14]. Public Cloud is less secure because of its openness and accessibility of general public.

Public Cloud comes with the features of flexibility, reliability, location independence, highly scalable and moreover cost efficient. On the other hand, it is less secure and less customizable.

ii. Private Cloud

Private Cloud allows systems and services to be accessible within the organization. It is more secure than Public Cloud because its resources are only shared within the organization.

It gives more control over services and provides more security with efficient energy. But it has only restricted area of operations with limited scalability [15]. It is also more costly because of its more control over the services. Private cloud also requires additional skills to manage the cloud.

iii. Community Cloud

Community cloud allows system and services to be accessible within the group of an organization. It shares the same infrastructure among different organizations from a certain community having a common vision [16]. Community Cloud can be managed internally by organizations or by any third party.

It is cost effective and secure. It also provides the facility of sharing the resources among different organizations. Since all the data is located at one place, so while placing the data in community cloud one should be more careful as it can be also accessible by others. On the other hand, it is also a challenging task to allocate the responsibilities of governance, security and cost among different organizations. As living in Community Cloud you have to face the networking issues and security compliance as you are living in both Public and Private cloud [17]. And it is also Infrastructure dependent.

iv. Hybrid Cloud

Hybrid Cloud is a mixture of both Public and Private cloud allowing its users to perform major or critical activities using Private Cloud while non- critical activities can be performed publically through Public Cloud [18]. It contains the features of both Public and Private cloud as Hybrid cloud is flexible, scalable, secure and cost efficient. According to the survey the Response

Over the years, the adoption of cloud services has an increasing trend for all three types of cloud deployment models including Public, Private and Hybrid cloud models. A comparison of cloud services adoption in 2020 vs. 2021 is shown in Fig.2.

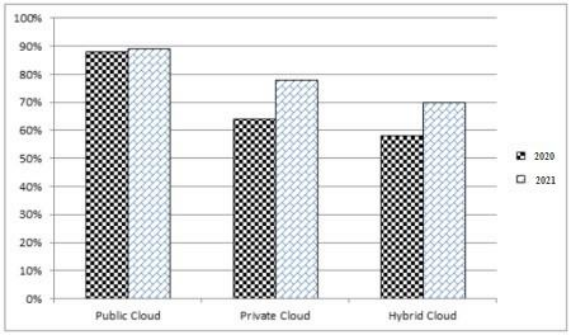

Fig. 2: Adopting Cloud Services in 2020 vs 2021

Because of its openness, pool of resources and services which are accessible anywhere and anytime, Cloud Computing has shown numerous positive effects in the field of IT. But as with the enhancement in IT industry, the Cloud Computing has many worthy advantages; but still we cannot deny with its weaknesses. Traditional security issues are still present in cloud and as from consumer's perspective, security of data is still a major issue and it is a barrier in adaptation of Cloud Computing.

C. Challenges in Cloud Computing

Consumer faces several issues while dealing with Cloud Computing. The common challenges are:

- Security is the major concern when data is placed on cloud as the cloud providing company or any shared user or customer can attack on server and information may be stolen.
- Personally Identifiable Information (PII) or any sensitive information of any customer which is shared with different organizations [19], there is a chance of Data leakage therefore assigning user privileges is also very crucial.
- The cloud user is completely unaware of the data location while placing it on cloud. The customer doesn't know that where its Data has been placed which refers to the unawareness of the locality of user's data.
- Many customers require services to be available all the time and downtime of server when the server is busy, may causes a barrier in the availability of services.
- Data need to be monitored so that any customer may not store illegal or inappropriate data on cloud [20] which points towards the data investigation.
- Many applications are data insensitive and ubiquitous mobile devices creates sensory overload of data because of such applications [21]. Transfer of such large amount of data creates bottleneck because of which services got suspended. Bottleneck causes delay in services.

- Cloud Service providers do not allow foreign inspection, and are willing to install new security certificates which requires regulatory compliance.
- Data of several users on cloud is also shared among those users who use the services of those service providers, so data segregation is also crucial.
- Due to any natural disaster (flooding, tsunami, earthquake etc.) or any other haphazard condition, the server may damage and data may loss.
- The cloud providing companies architects the infrastructure such that if ever after customer wants to switch to another cloud providing company, they cannot shift all their data to another cloud providing company. At this time the user become platform dependent.
- All the data placed on cloud by the customer is being replicated. If the user deletes the whole data there is still a copy of that data stored on server. So, there is always a chance on misuse and leakage of that data.

D. Issues in Cloud Computing

Security Issues

The reason why most of the organizations and customers resist shifting on cloud is because of Security and Privacy threat. As Cloud is not secure because of hackers and attackers. Some issues related to Security are:

- As the data is not stored on client computers and it stored or servers, because of any mishap if the data is lost from server all the data from client may also lost as they are directly accessing the server.
- Cloud Service providers show all the software and applied interface which is being shared among all the customers is same. Monitoring, sorting, authentication and access control is held by the service providers which in managed by the interface [22]. And any insecure interface may result in threat of data loss.
- Cloud does not provide separate resources and services to an extent because of which all the customers are accessing and utilizing the same technology. This shared technology also increases the threat of privacy.
- As we discussed, data is shared among different organizations and there may be a chance of misuse of information by any other employee of organization [23] because of any malicious insider.
- Customers get services through cloud via continuous sending request and in response the server responds means server and customer requires continuous communication. The attacker may arise certain big questions and send to the server, in result server may get busy and may not respond on time which cause flooding attacks.
- In Distributed Denial of Service (DDOS) Attack, an attacker intentionally or unintentionally generates traffic of so many requests on server in that duration of time, through different smart devices or computers and due to specific processing power of server it does not respond on time or even may crash. If the traffic is generated intentionally then it is an attack and the attacker may steal some data while server is down.
- The concept of Virtualization is that multiple users or tenants access single physical instance. Virtualization technique is based on assigning logical name and a pointer to every physical resource. Security of these virtual machines can be reduced by using some viruses and destructive softwares, such as rootkits. Rootkits are a set of computer software, which control a computer system. In Rootkit attack, the user did not notice the presence of rootkit and hacker can change all the settings of user's computer. This is a type of VM-Ware Based Malware Attack.

Privacy Issues

Major issue of Cloud is Data privacy because the data of all the users is centralized on a cloud server and they are connected through Cloud Services to access them. This information can be of any type, private photos, financial statements and regular files however personal information is considered as privacy of the respective person. Some important issues regarding privacy are discussed and presented below:

- When customer uses cloud, they store their information on Cloud by accessing Cloud Services. Later on if the customer wants to switch to any other cloud service provider, there is always a threat of unauthorized use of the critical information stored on the cloud. Moreover, many times it becomes very hard for the user to change its cloud service provider because a lock-in condition arises; at that point loss of control situation occurs.
- When user stores data on Cloud and do not have access to that data because of some issues. There is always a chance of access to the stored information on Cloud by an unauthorized person because of the lack of accessibility of authorized person [24].
- As the user is unaware of the locality of storage of data, the data can be stored on inappropriate storage space. The Cloud service providers have to pay less if the data is being stored on inappropriate places and it minimizes the cost of service providers hence increases their profit.

- When the data is stored on cloud, several replicas of data are made to facilitate the user in case of any unwanted data loss. But there is a threat of loss of that copy of data or of being threatened by that copy of data in future if user wants to take services from any other cloud service provider.
- The information of the unique devices such as IP addresses can be tracked.
- The information about digital content, social interactions, users accessing the website, computer, input and output devices which are connected also being gathered on the cloud.
- The sensitive information about the user and organization such as religion, financial transactions, financial statements, religion and job information is also being stored on cloud which may be misused in any aspect [25].
- Personal information about the individual related to personal identity which includes name, address, contact number, person's location, credit card number and zip code etc. are also being monitored.

Data Storage Issues

Trust is very important issue in storing data on cloud. Handing over of all the data to cloud service provider which act as intermediary party, is an important issue. Some check points which provide reliability to these centers are discussed below:

- The risk of theft of data can be minimized but can never completely disappear. Security providers are trying to reduce these issues by applying certain security measures on authentication and encryption methods of exchanging and storing information.
- By splitting the user's information from one server to multiple servers having different locations, with the help of virtual technology, the service providers are trying to protect the user's privacy.
- Transfer of data from one place to another and it's the splitting of data at different server's takes place at so much speed that the customer doesn't understand its original location of data storage.
- Multi-platform support makes it helpful for the user to access the cloud server on any sort of device. The cloudy system is fully virtualized and supports all kinds of OS [26] which means you can access same cloud services on any platform like Windows, Mac, Android, Linux and many more.
- One of the major concerns with respect to the security of data is integrity of data which concerns that data should remain unchanged. Data should remain in the condition as the customer wants to store it. Server or any third party may not be able to alter the data. Cloud service provider need to be aware of data integrity and ability to respond it.
- Due to any haphazard, natural and unnatural conditions data may not be available. To avoid this, user is recommended a copy of data in their own systems for the purpose of data recovery.
- All the services on Cloud are being accessed through Internet so there is a need of fast and reliable internet connection [27]. But in some cases if the user doesn't have internet access or due to some other issues cannot go online and access the cloud, the offline web services are provided and as the user gets connect with the internet all the data is made online on cloud. Through this a gap is not generated.
- User is also concerned about the transmission of Data, because it is dependent on the recovery format of cloud services companies and transmission of data and data conversion [28].

E. Principles of Data Security

Confidentiality, Integrity and Availability (CIA) is used in all security techniques of Data [29]. Confidentiality means the data is only available to authorized people. Integrity refers to high quality, accuracy, consistence and accessibility of data and the principle of availability refers to the data that should be available whenever it is needed by authorized users.

According to the analysis, the nine key principles of Data Security are given below [30].

1. Security Safeguards
2. Limiting the use by disclosure and retention
3. Responsibility
4. Purpose
5. Accept
6. Precision
7. Minimization
8. The openness, transparency
9. Integrity, license, power

III. PROPOSED FRAMEWORK

In this section, we introduce the framework of our proposed scheme. The framework is a Multi-Layer Token Framework (MLTF) which has three layers. These layers are elaborated in Fig.3.

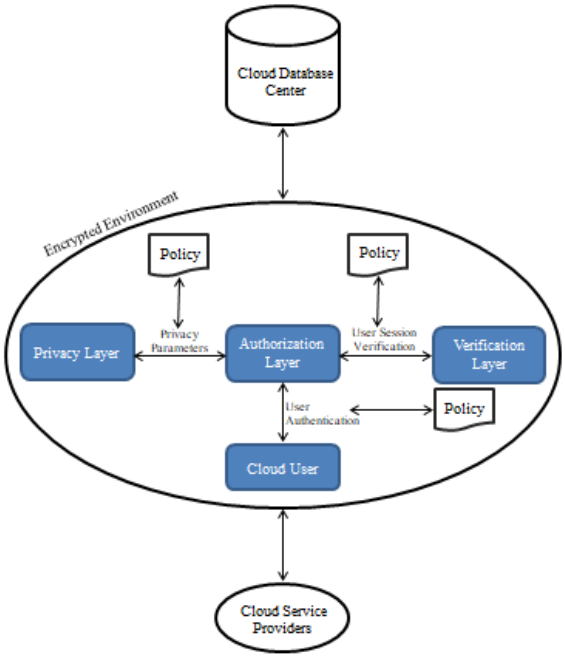

Fig. 3: Multi-Layer Token Framework

IV. Algorithms Over Different Layers

Proposed research constitutes three layers for data protection named as authorization layer, privacy layer and verification layer whose working is as below:

1. *Authorization Layer*
   This layer deals with two sections which are:
   - User SignUp
   - User LogIn
2. *Privacy Layer*
   This layer deals with two conditions which determine:
   - Condition I (Run when the token validates)
   - Condition II (Run when the token doesn't validates)
3. *Verification Layer*
   This layer verifies whether the data which is being accessed by any user has the authority to access it or not.

Algorithm for Authorization Layer				
Step	**Description**	**Input**		**Output**
User Sign-Up				
1.	Encrypt user password with SHA256 algorithm	User's password	→	Encrypted password
2.	Assign unique key (K_U) to user	None	→	User's key (K_U)
3.	Encrypt (K_U)with OpenSSL Get Cipher Methods algorithm	User's key (K_U)	→	Encrypted key (K_U^E)
User Login				
1.	Get Username of User	Username	→	User ID (ID)
2.	Get and Encrypt user password with SHA256 algorithm	User's password	→	Encrypted password (P^E)
3.	Concatenating Access Time	getCurrentTime()	→	Access Time (AT)
4.	Generate token (T) when user logs in	($ID + P^E + AT$)	→	Token (T)
5.	Generate initial (T_i) token by Encrypting the T and use it as a key	T^E	→	Initial token (T_i)
6.	Concatenate T_i with K_U^E using OpenSSL Get Cipher Methods algorithm to generate final token (T_f)	($T_i . K_U^E$)	→	Final token (T_f)

Algorithm for Privacy Layer				
Step	**Description**	**Input**		**Output**
1.	Validate token (T_f)	Requested data + T_f	→	True if token is valid, False otherwise
2.	Check if requested data is allowed	Requested data	→	Acknowledged data if allowed, Error message if not allowed
3.	Fetch requested data from Cloud DB Center	Requested data	→	Data from database
4.	Show requested data to user	Data from database	→	Displayed data to user

Algorithm for Verification Layer				
Step	**Description**	**Input**		**Output**
1.	Record transaction based on T_f	Requested data, T_f	→	Transaction code
2.	Generate OK code if requested data is allowed	Requested data	→	OK code
3.	Generate suspicious activity code 404 if requested data is not allowed	Requested data	→	Suspicious activity code 404

V. Proposed Token Generation Algorithm

In this section, we present the token generation algorithm and discuss its various steps.
When user SignUp in the system by using password; its password is encrypted with SHA256 Algorithm named as (P^E). At that time a Key (K_U) is assigned to the user by Cloud Administrator. Then, the user key is encrypted with OpenSSL Get Cipher Methods Algorithm which results in Random Key (K_U^E).
When User Logs In; a token (T) is generated by using the parameters of UserID, Encrypted Password and Access Time ($ID + P^E + AT$). That encrypted token (T^E) is entitled as Initial Token as (T_i) which is generated with SHA256 Algorithm. At last, final

token (T_f) is generated by concatenating T_i with K_U^E using OpenSSL Get Cipher Methods algorithm.

$T_f = T_i \,.\, K_U^E$

$T_f = (IDP^E AT)^E \,.\, K_U^E$

Algorithm for Proposed Token Generation				
Step	**Description**	**Input**		**Output**
1.	Encrypt the user's password using SHA256 Algorithm to get the encrypted password PE.	User's password	→	Encrypted password ($\boldsymbol{P^E}$)
2.	Assigns a random key to the user ($\boldsymbol{K_U}$) by the Cloud Administrator.	--	→	Random Key assigned by Cloud Administrator ($\boldsymbol{K_U}$)
3.	Generates a random key ($\boldsymbol{K_U^E}$) and encrypt it using OpenSSL Get Cipher Methods Algorithm.	--	→	Encrypted Random Key ($\boldsymbol{K_U^E}$)
4.	When the user logs in, it generate a Token ($\boldsymbol{T}$) using ($\boldsymbol{ID.P^E.AT}$).	($\boldsymbol{ID.P^E.AT}$)	→	Token ($\boldsymbol{T}$)
5.	Generate initial token $\boldsymbol{T_i}$ by Encrypting the token $\boldsymbol{T}$ and use it as a key	($\boldsymbol{T^E}$)	→	Initial token ($\boldsymbol{T_i}$)
6.	Returns the final token ($\boldsymbol{T_f}$) by concatenating $\boldsymbol{T_i}$ with $\boldsymbol{K_U^E}$ using OpenSSL Get Cipher Methods algorithm.	($\boldsymbol{T_i.K_U^E}$)	→	Final token ($\boldsymbol{T_f}$)

VI. Parameters of Proposed Technique

The MLTF framework is comprised of various parameters over the user level and cloud administrative level. The parameters of Data Confidentiality, Privacy Protection, Access Control, Trust, and Governance are considered for both levels. Whereas, User Authentication is considered for only User level, and Data Encryption is only considered for Administrator level. Table 1 shows the parameters of proposed framework over the user and administrator levels.

Table 1: Parameter of Proposed Framework

Feature	User Level	Administrator Level
User Authentication	√	
Data Confidentiality	√	√
Privacy Protection	√	√
Data Encryption		√
Access Control	√	√
Trust	√	√
Governance	√	√

VII. Result Discussion

In this section, we use Memory Cost, Time Cost and Resource Cost as performance metrics which are calculated on the basis of different types of token. We use three types of tokens for authentication and authorization as given below:

i) Token Generated on the behalf of UserID, Password

ii) Token Generated on the behalf of UserID, Password + AccessTime

iii) Token Generated on the behalf of UserID & Password + AccessTime + Key

The performance metrics are elaborated as:

Memory Cost is the memory being occupied by the token when it is generated.

Time Cost is the time consumed by the token when it is generated. And the time is calculated in milliseconds.

Resource Cost is the amount of resources being used by the token.

Token Generated By User ID

Memory Cost (KB): 1024

Time Cost (ms): 3.8788318634033

Resource Cost: 2

Token Generated By User ID and Access Time

Memory Cost (KB): 1024

Time Cost (ms): 4.7421455383301

Resource Cost: 2

Token Generated By User ID and Access Time and Key

Memory Cost (KB): 1024

Time Cost (ms): 5.6900978088379

Resource Cost: 2

Fig. 4: Values of Memory Cost, Time Cost and Resource Cost of Token

The values of Memory Cost, Time Cost and Resource Cost of the system occupied by token keeps on changing every time the token is generated because the system is not in a static state and its state keeps on changing. The instantaneous values of the performance matrices for three different types of tokens are shown in Fig.4.

Percentages of simulated data have been taken to demonstrate the results on behalf of three differently generated tokens as there is no certain rule to measure the privacy. Tracy Ann Kosa et al., 2013 mentioned that there is no cohesive theory of privacy. Economics, Political Sciences, Law, Philosophy and

Sociology thoroughly explores the concept of privacy whereas Computer Science has attempted to apply the concept of privacy with varying degrees of success. Similarly Privacy Impact Assessment (PIA) deals with privacy of personal data and solutions to safeguard it, International Association of Privacy Professionals (IAPP) and General Data Protection Regulation (GDPR) states that privacy can be improved through different tactics but it cannot be measured.

Thus, a comparison is made at different cloud servers to compare the token generation time of different specifications of systems with the minimum and maximum systems attached with the cloud server.

i) Token Generation Time with minimum number of systems attached on Cloud Servers

The time taken to generate the token for minimum number of systems attached to different cloud servers with various system specifications are given in Table 2.

1. Minimum 1 system can be attached with the cloud server localhost of following specifications takes about 0.3ms to generate a token.
2. Normally, 5 systems are attached at its minimum with the cloud server http://62.171.141.159/test.php of following specifications takes about 0.4ms to generate their tokens.
3. Normally, 7 systems are attached at its minimum with the cloud server http://172.107.33.6/test.php of following specifications takes about 1.9ms to generate their tokens. And so on.

Table 2: Token Generated on Cloud with Minimum Numbers of Systems Attached

No. of PC	System Specifications		Token Generation Time (ms)	Cloud Server	Min No. of Systems Attached
	CPU	RAM			
1	corei7	16GB	0.3	local host	1
2	Intel Xeon E5-2630 v4	16 GB	0.4	http://62.171.141.159/test.php	5
3	Intel Xeon E5-2690 v2	16GB	1.9	http://172.107.33.6/test.php	7
4	Intel Xeon E5-2630 v4	30 GB	0.3	http://5.189.134.45/	3
5	AMD 16 core	30GB	0.2	http://103.164.54.23/test.php	12
6	Intel Xeon E5-2630 v4	30 GB	0.3	http://161.97.68.18/test.php	18
7	AMD 16 core	30GB	0.1	http://209.126.5.182/test.php	2
8	AMD 16 core	30GB	0.5	http://173.249.47.10/test.php	9
9	AMD 16 core	30GB	0.2	http://161.97.169.95/test.php	4
10	AMD 16 core	16GB	0.2	http://161.97.169.95/test.php	6

The token generation time with respect to minimum number of systems attached over cloud is shown in Fig.5.

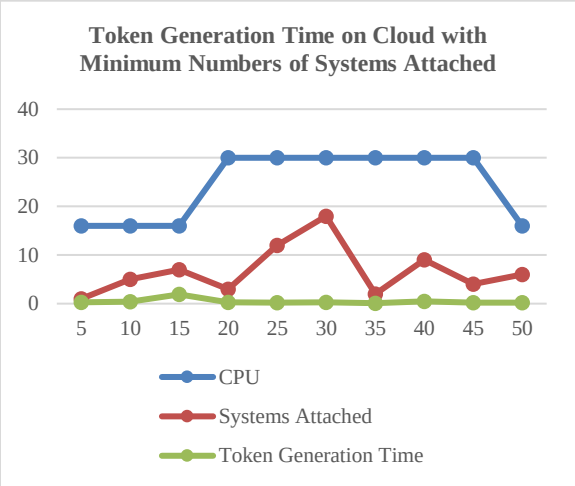

Fig. 5: Token Generated on Cloud with Minimum Number of Systems Attached

ii) Token Generation Time with maximum number of systems attached on Cloud Servers

The time taken to generate the token for maximum number of systems attached to different cloud servers with various system specifications are given in Table 3.

1. Maximum 1 system can be attached with the cloud server localhost of following specifications takes about 0.3ms to generate a token.
2. 18 systems can be attached at its maximum with the cloud server http://62.171.141.159/test.php of following specifications takes about 0.4ms to generate their tokens.
3. 32 systems can be attached at its maximum with the cloud server http://172.107.33.6/test.php of following specifications takes about 4.9ms to generate their tokens. And so on.

Table 3: Token Generated on Cloud with Maximum Number of Systems Attached

No. of PC	System Specifications		Token Generation Time (ms)	Cloud Server	Max No. of Systems Attached
	CPU	RAM			
1	corei7	16GB	0.2	local host	1
2	Intel Xeon E5-2630 v4	16 GB	2.0	http://62.171.141.159/test.php	18
3	Intel Xeon E5-2690 v2	16GB	4.9	http://172.107.33.6/test.php	32
4	Intel Xeon E5-2630 v4	30 GB	1.7	http://5.189.134.45/	11
5	AMD 16 core	30GB	4.9	http://103.164.54.23/test.php	25
6	Intel Xeon E5-2630 v4	30 GB	3.6	http://161.97.68.18/test.php	30
7	AMD 16 core	30GB	2.1	http://209.126.5.182/test.php	15
8	AMD 16 core	30GB	7.3	http://173.249.47.10/test.php	40
9	AMD 16 core	30GB	4.7	http://161.97.169.95/test.php	19
10	AMD 16 core	16GB	3.1	http://161.97.169.95/test.php	32

The token generation time with respect to maximum number of systems attached over cloud is shown in Fig.6.

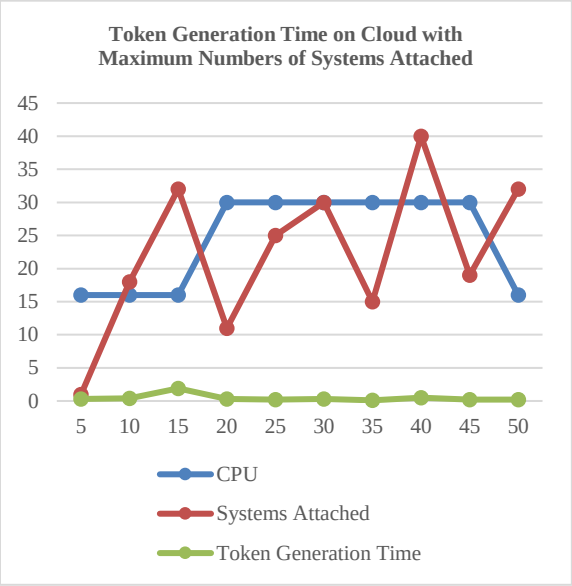

Fig. 6: Token Generated on Cloud with Maximum Numbers of Systems Attached

VIII. Features and Strengths of Proposed Technique

The performance of the proposed MLTF framework is demonstrated with different features and strengths. The key features are User Authentication (i.e., only authenticate user can login), Multi-Layer model (i.e., specific rights are given to the user), Key (i.e., a random key is assigned to the user upon registration), Token Generation (i.e., a token is generated for each user to track her activities), Encryption (i.e., data is encrypted at cloud), and Code Generation (i.e., a specific code is generated for each activity of the user). A summary of key features and their corresponding strengths is given in Table 4.

Table 4: Features and Strengths of Proposed MLTF Framework

Feature	Strength
User Authentication	Only authentic users can perform the activities over the cloud network.
Multi-Layer	Specific privileges are assigned to the user and they can only perform the underprivileged activities.
Key	Random key is assigned to the user when it gets register.
Token Generation	The token is generated for every user to keep track the activities of the users. So that the record of the activities of the user may kept.
Encryption at cloud level	All the data stored at cloud is encrypted so there is no threat of privacy of data.
Code Generation	A code is generated on the base of activities performed by the user.

IX. Conclusion

The data sensitivity, security, privacy, and secrecy of cloud users are of vital importance. We proposed an adequate framework which mitigates the theft of data and makes the data more private. The framework achieves security and privacy through multi-layer token. The layered approach applied attributes on sensitive data and passes it through three layers of security policies including authorization, security, and privacy. And the token generated on behalf of userID, Password, AccessTime, and Key which enters the users in a better and protected environment of Cloud Computing. The proposed scheme outperformed in terms of data confidentiality, privacy protection, data encryption, access control, trust and governance at both user and administrator levels. The add-on of the proposed method with higher number of layers and increased number of performance matrices needs to be further explored in future.

References

[1] Veeramanickam M. R. M. and Mohanapriya M., "Research paper on E-Learning application design features: Using cloud computing & software engineering approach," *2016 Int. Conf. Inf. Commun. Embed. Syst.*, no. Icices.

[2] Sharma P. S., "Mobile Cloud Computing : Its Challenges and Solutions," vol. 4, no. 5, pp. 287–293, 2015.

[3] Yan Z. et al. , "Heterogeneous Data Storage Management with Deduplication in Cloud Computing," *IEEE Trans. Big Data*, no. 2, pp. 1–1, 2017.

[4] A. Sunyaev, "Cloud Computing," *Springer Nature Switzerland AG 2020.* , https://doi.org/10.1007/978-3-030-34957-8_7

[5] Aski et al., "An Authentication-Centric Multi-Layered Security Model for Data Security in IOT-Enabled Biomedical Applications." *2019*

IEEE 8th Global Conference on Consumer Electronics (GCCE),2019, https://doi.org/10.1109/gcce46687.2019.9015217.

[6] Kara, Mostefa, et al. *One Digit Checksum for Data Integrity Verification of Cloud-Executed Homomorphic Encryption Operations*. 2023.

[7] Tran H. V., "Data management challenges in cloud computing," *Proc. 13th Int. Conf. Comput. Sci. Its Appl. ICCSA 2013*.

[8] Otieno, Martin. "Techniques and Protocols for Enhancing Data Privacy in Cloud Computing: A Review." *World Journal of Advanced Engineering Technology and Sciences*, vol. 8, no. 1, 2023, pp. 391–404, https://doi.org/10.30574/wjaets.2023.8.1.0064.

[9] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(12). https://doi.org/10.1007/s11227-020-03213-1

[10] Chen D. and Zhao H., "Data Security and Privacy Protection Issues in Cloud Computing," *2012 Int. Conf. Comput. Sci. Electron. Eng.*, no. 973.

[11] Sunyaev, A. (2020). *Internet computing: principles of distributed systems and emerging internet-based technologies*. Cham, Switzerland: Springer.

[12] Alouffi, Bader, et al. "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies." *IEEE Access*, vol. 9, 2021, pp.57792–57807., https://doi.org/10.1109/access.2021.3073203.

[13] Slimani, Sarra, et al. "Service-Oriented Replication Strategies for Improving Quality-of-Service in Cloud Computing: A Survey." *Cluster Computing*, 4 May 2020, https://doi.org/10.1007/s10586-020-03108-z.

[14] Arjun and Vinay, (2016). "A Short Review on Data Security and Privacy Issues in Cloud Computing," *IEEE*.

[15] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Davila Delgado, J. M., Akanbi, L. A., … Owolabi, H. A. (2020). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.sciencedirect. https://doi.org/10.1016/j.autcon.2020.103441

[16] Hakak S., "A Review on Mobile Cloud Computing and Issues in it," vol. 75, no. 11, pp. 1–4, 2014.

[17] Mulder, Jeroen. *Multi-Cloud Architecture and Governance*. Packt Publishing Ltd, 11 Dec. 2020.

[18] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*,102642. https://doi.org/10.1016/j.jnca.2020.102642

[19] *Privacy Impact Assessment for CBP One™*. 2021.

[20] Ruan A. and Martin A., "RepCloud: Attesting to Cloud Service Dependency," *IEEE Trans. Serv. Comput.*, vol. 10, no. 5, pp. 675–688, 2017.

[21] Sinha N. and Khreisat L., "Cloud Computing Security , Data , And Performance Issues," *IEEE*, pp. 1–6, 2014.

[22] AL-Jumaili, Ahmed Hadi Ali, et al. "Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations." *Sensors*, vol. 23, no. 6, 8 Mar. 2023, p. 2952, https://doi.org/10.3390/s23062952.

[23] Yu T. and Zhu Y.-G., "Research on Cloud Computing and Security," *11th Int. Symp. Distrib. Comput. Appl. to Business, Eng. Sci.*.

[24] Dorairaj, S. D., & Kaliannan, T. (2015). An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment. *The Scientific World Journal*, *2015*, 601017. https://doi.org/10.1155/2015/601017

[25] Anandaraj S. P. and Kemal M., "Research Opportunities and Challenges of Security Concerns associated with Big Data in Cloud Computing," *Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud) (I-SMAC 2017)*.

[26] Daffu P. and Kaur A., "Mitigation of DDoS attacks in cloud computing," *5th Int. Conf. Wirel. Networks Embed. Syst. WECON 2016*.

[27] Ali O. et al., "Challenges and issues that are perceived to influence cloud computing adoption in local government councils," *Proc. 2017 IEEE 21st Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2017*.

[28] Dinadayalan P., et al. (2014). "Data security issues in cloud environment and solutions," *Proc. - 2014 World Congr. Comput. Commun. Technol. WCCCT 2014*, pp. 88–91.

[29] Awaysheh, F., Cabaleiro, J. C., Pena, T. F., & Alazab, M. (2019). Big Data Security Frameworks Meet the Intelligent Transportation Systems Trust Challenges. *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. https://doi.org/10.1109/trustcom/bigdatase.2019.00117

[30] Mahdi Shariati S. et al., "Challenges and security issues in cloud computing from two perspectives: Data security and privacy protection," *2nd Int. Conf. Knowledge-based Eng. Innov.*