Application of Dynamic Token Check Technique in Cloud Computing

Okoronkwo, Madubuezi C.

***Abstract*— Cloud computing is the newest tool in the Information and Communication Technology and business activity at present. It is another internet based technology where the users can subscribe high quality of services from data and software that inhabits in the remote servers. It is an internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Its rising network bandwidth and dependable network connections make it achievable that clients can at present subscribe high superiority services from data and software that inhabit exclusively on isolated data cores. The reliance management among data owners and storage services providers is the critical dilemma in cloud security, which burden for an efficient prerequisite of data handling. In this research, dynamic token check technique is recommended to guard public data objects and extremely dispersed software modules. These techniques protect user authentication and stiffen the data access-control in open clouds.**

***Index Terms*— Cloud, Computing, Internet, Security, Data**

I. INTRODUCTION

Cloud computing has been imagined as the next generation information technology architecture for endeavors. It means a remote server that is accessed through the internet which helps in business applications and functionality add-ins alongside with the usage of computer software [1]. The cloud of services and applications in the internet modem is available from the computer. Cloud computing helps in logging in to the computer applications you need. With Cloud Computing, one can enjoy web services, sales force or office computerization programs, blog sites, spam filtering, data storage services, etc. Cloud servers are not only used to store data like a ware house , it also provides frequent updates on data by the users with different operations like insert, delete , update and append. It provides three types of services i,e., Infrastructure as a service(IaaS) , Platform as a service(PaaS) and Software as a service(SaaS) [2]. End users access the cloud based applications through the web browsers with internet connection. Moving data to clouds makes more convenient and reduce to manage hardware complexities. Data stored at clouds are maintained by Cloud service providers (CSP) with various incentives for different levels of services. Moving data into the cloud proffers enormous ease to users since they don't have to concern about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. Despite the fact that there is an advantage of accessing the data from the remote servers there raises a security problem. Data stored at clouds are maintained by Cloud service providers (CSP) with a variety of motivations for different levels of services. Nevertheless it eradicates the dependability of local machines to retain data, there is a chance to lose data or it effects from external or internal attacks. In order to surmount the hitch, we proposed a resourceful and valuable method to guarantee the integrity and availability of the data using dynamic token check technique.

Manuscript received October 21, 2014.
Okoronkwo, Madubuezi C., M.Sc., Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria

II. HISTORICAL BACKGROUND

The underlying concept of cloud computing dates to the 1950s, when large-scale mainframe computer were seen as the future of computing, and became available in academia and corporations, accessible via thin clients computers, often referred to as "static terminals", because they were used for communications but had no internal processing capacities. To make more efficient use of costly mainframes, a practice evolved that allowed multiple users to share both the physical access to the computer from multiple terminals as well as the CPU time [3]. This eliminated periods of inactivity on the mainframe and allowed for a greater return on the investment. The practice of sharing CPU time on a mainframe became known in the industry as time-sharing. During the mid 70s, time-sharing was popularly known as Remote Job Entry; this nomenclature was mostly associated with large vendors such as IBM and DEC. In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service, but at a lower cost. By switching traffic as they saw fit to balance server use, they could use overall network bandwidth more effectively [4]. They began to use the cloud symbol to denote the demarcation point between what the providers was responsible for and what users were responsible for. Cloud computing extends this boundary to cover all servers as well as the network infrastructure. As computers became more prevalent, scientists and technologists explored ways to make large-scale computing power available to more users through time-sharing. They experimented with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users. In early 2008, Eucalyptus became the first open-source, AWS API-compatible platform for deploying private clouds. In early 2008, OpenNebula enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid

clouds, and for the federation of clouds [5]. In the same year, efforts were focused on providing quality of service guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting in a real-time cloud environment. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them and observed that organizations are switching from company-owned hardware and software assets to per-use service-based models, so that the projected shift to computing will result in dramatic growth in IT products in some areas and significant reductions in other areas. In July 2010, Rackspace Hosting and NASA jointly launched an open-source cloud-software initiative known as OpenStack [5]. The OpenStack project intended to help organizations offer cloud-computing services running on standard hardware. The early code came from NASA's Nebula platform as well as from Rackspace's Cloud Files platform. On March 1, 2011, IBM announced the IBM SmartCloud framework to support Smarter Planet. Among the various components of the Smarter Computing foundation, cloud computing is a critical piece [6]. On June 7, 2012, Oracle announced the Oracle Cloud. While aspects of the Oracle Cloud are still in development, this cloud offering is posed to be the first to provide users with access to an integrated set of IT solutions, including the Applications (SaaS), Platform (PaaS), and Infrastructure (IaaS) layers.

III. Service Models

Once a cloud is recognized, how its cloud computing services are deployed in terms of business models can diverge depending on necessities. The primary service models being deployed are commonly known as:

i. Software as a Service (SaaS)

Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud. Also, Microsoft is expanding its involvement in this area, and as part of the cloud computing option for Microsoft® Office 2010, its Office Web Apps are available to Office volume licensing customers and Office Web App subscriptions through its cloud-based Online Services.

ii. Platform as a Service (PaaS)

Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed.

iii. Infrastructure as a Service (IaaS)

Consumers control and manage the systems in terms of the operating systems, applications, storage, and network connectivity, but do not themselves control the cloud infrastructure.

Also known are the various subsets of these models that may be related to a particular industry or market. Communications as a Service (CaaS) is one such subset model used to describe hosted IP telephony services. Along with the move to CaaS is a shift to more IP-centric communications and more SIP trunking deployments. With IP and SIP in place, it can be as easy to have the PBX in the cloud as it is to have it on the premise. In this context, CaaS could be seen as a subset of SaaS. Figure 1 shows the configuration in a cloud computing environment.

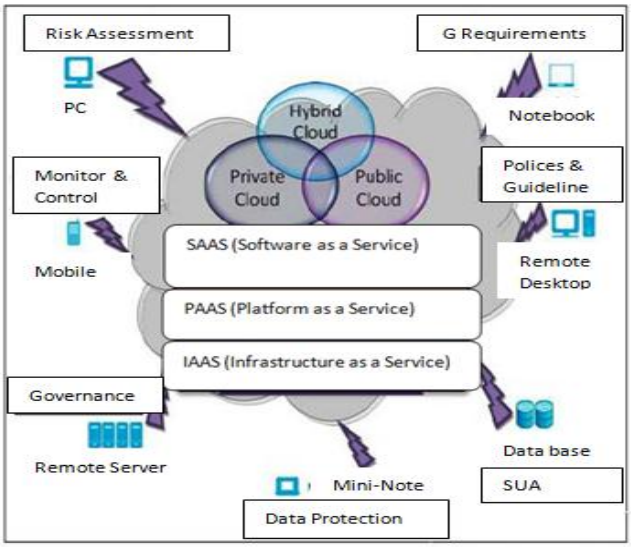

Figure1: Cloud computing environment.

3.1. Characteristics Cloud computing

Cloud computing exhibits the following key characteristics:

i. Agility improves with users' ability to re-provision technological infrastructure resources.

ii. Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way that a traditional user interface (e.g., a computer desktop) facilitates interaction between humans and computers. Cloud computing systems typically use Representational State Transfer -based APIs.

iii. Cost reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state-of-the-art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Iv. Device and location independence enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

v. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

vi. Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

a. centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

b. peak-load capacity increases (users need not engineer for highest possible load-levels)

c. utilisation and efficiency improvements for systems that are often only 10–20% utilized.
vii. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
viii. Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.
ix. Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
x. Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis in near real-time, without users having to engineer for peak loads.
xi. Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

3.2. Benefits cloud computing

The following are some of the possible benefits for those who offer cloud computing-based services and applications:
i. Cost Savings: Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
ii. Scalability/Flexibility: Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.
iii. Reliability: Services using multiple redundant sites can support business continuity and disaster recovery.
iv. Maintenance: Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
v. Mobile Accessible: Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

3.3. Challenges in cloud computing

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a Slow down when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.

a. Security and Privacy

Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.

b. Lack of Standards

Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.

c. Continuously Evolving

User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

d. Compliance Concerns

The Sarbanes-Oxley Act (SOX) in the US and Data Protection directives in the EU are just two among many compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. The EU has a legislative backing for data protection across all member states, but in the US data protection is different and can vary from state to state. As with security and privacy mentioned previously, these typically result in Hybrid cloud deployment with one cloud storing the data internal to the organization.

3.4. Security in the Cloud Computing

If we wish to enable cloud-driven growth and innovation through security, we must have a clear framing on what is meant by security. Security has been notoriously hard to define in the general case. The canonical goals of information security are Confidentiality, Integrity, and Availability. We borrow from NIST to include Accountability and Assurance, and then add a sixth category of Resilience. We define these terms below and map them to the cloud context, with a few examples of how they can be supported by both technical and non-technical mechanisms.

a. Confidentiality

Confidentiality refers to keeping data private. Privacy is of great importance as data leaves the borders of the organization. Not only must internal secrets and sensitive

personal data be safeguarded, but metadata and transactional data can also leak important details about firms or individuals. Confidentiality is supported by, among other things, technical tools such as encryption and access control, as well as legal protections.

b. Integrity

Integrity is a degree confidence that the data in the cloud is what is supposed to be there, and is protected against accidental or intentional alteration without authorization. It also extends to the hurdles of synchronizing multiple databases. Integrity is supported by well audited code, well-designed distributed systems, and robust access control mechanisms.

c. Availability

Availability means being able to use the system as anticipated. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement.

d. Accountability

Accountability maps actions in the system to responsible parties. Inside the cloud, actions must be traced uniquely back to an entity, allowing for integration into organizational processes, conflict resolution and deterrence of bad behavior. Accountability is supported by robust identity, authentication and access control, as well as the ability to log transactions and then, critically, audit these logs.

e. Assurance

Assurance refers to the need for a system to behave as expected. In the cloud context, it is important that the cloud provider provides what the client has specified. This is not simply a matter of the software and hardware behaving as the client expects but that the needs of the organization are understood, and that these needs are accurately translated into information architecture requirements, which are then faithfully implemented in the cloud system. Assurance is supported by a trusted computing architecture in the cloud, and a by careful processes mapping from business case to technical details to legal agreements.

f. Resilience

Resilience in a system allows it to cope with security threats, rather than failing critically. Cloud technology can increase resilience, with a broader base, backup data and systems, and the potential identify threats and dynamically counteract. However, by shifting critical systems and functions to an outside party, organizations can aggravate resilience by introducing a single point of failure. Resilience is supported by redundancy, diversification and real-time forensic capacity.

IV. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

a. Access to Servers & Applications

In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections which are not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data.

b. Data Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications

c. Virtual Machine Security

Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in Para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems.

d. Network Security

Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc

e. Data security

For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In order to assure the information security and data integrity, Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are the most common adoption. In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However, in cloud computing, the enterprise data is stored outside the enterprise boundary, at the Service provider end. Consequently, the service provider must adopt additional security checks to ensure data security and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for data security and fine-grained authorization to control access to data.

f. Data Privacy

The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

g.Data Integrity

Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. Transactions should follow ACID (atomicity, consistency, isolation and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

h. Data Location

In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications.

i. Data Availability

Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

j. Data Segregation

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

k. Security Policy and Compliance

Traditional service providers are subjected to external audits and security certifications. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust. Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources. An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail.

l. Securing Data-Storage

Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact.

m. *Patch Management*

The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

4.1. Ensuring data storage over cloud

In cloud data storage system, users store their data remotely on clouds, so that the correctness and availability of data files must be guaranteed to be identical. Our aim is to detect the servers which behaves differently and may leads to internal and external threats. In this paper, we explore the technique used to detect the modified blocks easily with very less overhead using token pre-computation technique.

a. Challenge Token Pre-Computation

To realize data storage correctness and data integrity, we use an algorithm which takes a few parameters and compute the token. Token generation algorithm works as follows:

Let F be the filename and fL be the length of the file and V be the secret matrix which contains special characters in randomized order. Compute the key with the following parameters:

Algorithm Pre-Token Generation

Procedure

Choose parameters F, fL and secret vector V. Choose number of blocks to be taken (normally fixed block size)

X= F + fL + V

Compute key

for i=1 to n

fileToken =fileToken +(Σni=1 split(Xi))

Compute short signatures for each block of the file by considering Token and file block data using bit permutations (Token +block data) and store these values in client for dynamic checking End procedure

V. RESULTS

Before file is distributed to the cloud, TPA will generate token key with required parameters passed by user. once the token key has been generated, TPA will send the file by dividing the file into equal sized blocks and generate a small token signature for each block along with initial key file Token .This file Token was generated based on mathematical calculations with hash based technique, It is fully randomized we are not explore the operations present in it and just given the function split(X). Before sending the block it stores the computed signatures obtained from bit permutations on both file Token and block data .The resultant token was stored in its database or at clients place. Each block is send along with short signature and each block is treated as encrypted block. Cloud will perform the same operation and checks whether the given block is same or not when computed and checks with the signature. If it matches the same, cloud server store each block and acknowledges the newly generated signature to TPA.TPA verifies the signature with the existing signature, if it matches TPA will send next block otherwise it assumes that block was not saved successfully or it may effect to attacks and resend the same block

VI. CONCLUSION

In cloud computing, data security has always been an important aspect. In order to surmount the hitch, we proposed a resourceful and valuable method to guarantee the integrity and availability of the data using dynamic token check technique. By utilizing the dynamic token check, we can almost guarantee the simultaneous identification of the misbehaving server(s) and safeguarding our data in cloud environment.

REFERENCES

[1] Malden A. Vouk"Cloud computing –Issues, Research and Implementations", JCIT-CIT 16, 2008, 4,235-246.

[2] Luis M.Vaquero and Luis Rodero-Merino "A Break in the Clouds: Towards a Cloud Definition", AC SIGCOMM computer communication Review , volume 39, Number 1, January 2009.

[3]. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] Balachandra R. K and Ramakrishna P. V, "Cloud Security Issues", IEEE International conference on service computing, 2009

[5] Blumenthal, Marjory, "Is Security Lost in the Clouds?", Telecommunications Policy Research Conference, Oct 2, 2010.

[6] W. Li and L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", Cloud Computing, Proceedings on First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009, pp. 69-79.

Okoronkwo Madubuezi C. is currently a lecturer in Computer Science Department of Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. He has a Bachelor Degree in Computer Science from Michael Okpara University of Agriculture, Umudike, and a Master's Degree in Computer Science from Ebonyi State University, Abakaliki. He is presently pursuing a PhD programme in Computer Science from Nnamdi Azikiwe University, Awka, Anambra State of Nigeria with interest in System analysis, Design and Development. He is a member Computer Professionals of Nigeria