International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 7 July 2015

A Survey on Various Pre-calculate and Authentication Techniques

Tushar Mahale[1], Mr. Jitendra Dangra[2]
Dept. Of Computer Science and Engineering, Laxmi Narayan College of Technlogy, Indore, (M.P.) [1, 2]
tushar.mahale.be@gmail.com[1]

Abstract: *Cloud computing is a globalised concept and there are not any borders among the cloud. Computers used to process and store user knowledge may be settled any place on the world, depending on the supply of needed capacities within the international computer networks used for cloud computing. The information may be stored remotely within the cloud by the users and may be accessed using thin clients as and when needed. one of the main issue in cloud these days is Performance for outsourced storage is probably going to be lower than local storage and different major issue is knowledge security in cloud computing. Storage of data within the cloud may be risky because of use of internet by cloud primarily based services which suggests less management over the stored data. One amongst the main concern in cloud is however will we grab all the advantages of the cloud whereas maintaining quick accessing knowledge and security controls over the organizations assets.*

In future we will propose a new methodology Pre-calculated for storing data and also provide security in terms of authentication for stored data in clouds by using Cipher Text.

Keywords**:** c*loud computing, pre-calculete, authentication on cloud, security on cloud.*

1. Introduction

Cloud as defined by NIST [14]: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. Essential Characteristics:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

2. Literature Review

In this paper [1], Authors present a new approach, which allows calculation of word specific decision thresholds in advance. Starting with score distributions of phonemes, the cpdf's of keywords can be calculated and then applying different strategies decision thresholds can be fixed. Using only equal-length keywords, word specific decision thresholds don't become very effective. The advantageous application of word specific decision thresholds is the greater the more the vocabulary contains both short keywords and very long keyword-phrases. However, it may be promising to apply a specific kind of post-processing in order to avoid keyword overlaps and to consider statistically achieved regularities of the language.

In this paper [2], the novel method of *Jacobi Compensation* has been presented by authors, they allows modification of precalculated trajectories online during the robot gait. It is possible to shift parts of the robot in given cartesian directions of selected task coordinates thereby altering the posture of the humanoid to improve e.g. stability. This method can be used to modify precalculated gait trajectories in order to compensate for errors or adapt the trajectories in order to make them applicable to situations other than those they have been computed for.

In this paper [3], author had present simulation with a pre-calculated fluid simulator states (FSS) is based on partial computation with synchronous utilization of pre-calculated fluid simulator states stored on a disk device. This concept can drastically improve the simulation and subsequent visualization speed of wide computer graphics applications based on fluid simulator while keeping the preciseness of computation unchanged. Author have designed and implemented hierarchical tree structures built from pre-calculated fluid simulator states, which allow incremental, progressive and easy construction of various configurations of the boiler with high speed, interactive visualization and replaying of results.

In this paper [4], author had proposed a two-level distributed authentication architecture for wireless networks. Mobile hosts are using the Host Identity Protocol (HIP) to connect to the legacy Internet hosts through operator's WLAN. The system includes an operator-specific proxy server and a distributed firewall running directly on WLAN APs. Authors had implemented the system by reflashing the firmware of two different AP models with Linux-based OpenWRT distribution.

In this paper [5], author had designed a system that uses a Bluetooth mobile device to unlock doors in a fully automatic process with the possibility to reconfigure the system to work in semi-automatic mode to get the approval of the user if he input a PIN code as additional security procedure. The design fulfills the requirement as defined with fast and secured distribution of the keys compared to the physical keys with minimum possible requirements for the hardware, reasonable power consumption and support for tailored personalized keys. An authentication protocol, a key distribution and a key revocation method were proposed.

In this paper [6], author had shown the drawbacks in the existing authentication protocol. This paper proposes to improve the performance Group Registration technique based on hybrid mechanisms is proposed in this paper. It results in lesser bandwidth consumption and reduces the computation and communication cost. The proposed scheme can withstand the replay attack and the impersonating attack on mobile communications. According to the analysis of authors it was proved that the proposed method is not only secure against various known attacks, but also more efficient than previously proposed schemes.

In this paper [7] authors considered the Timing Covert Channel as a threat to network security, is exploited for identity authentication. Utilizing the packet intervals, authors implemented the TCC-based authentication on

the common FTP platform. The authentication tag is embedded into the packet intervals. The experiments show: 1) Their method is a secure way for authentication, since it is difficult to detect and decrypt the TCC authentication; 2) it could be implemented on many common network applications. In a word, the covert channel, such as TCC, can be a supplement for traditional authentication methods.

In this paper [8] author has given an image authentication watermarking scheme based on image segmentation and sharing mechanism is proposed. The scheme can resist VQ attack effectively because of the sensitiveness of segmentation algorithm. The authentication watermark can localize the alteration of the image contents, and the recovery data which are derived from different regions and embedded into the entire image, can almost restore the distorted regions effectively.

In this paper [9] author had designed Materialized Views to contribute in answering queries efficiently to improve the overall performance of Data Warehouse. Efficient query answering can further be speeded up by creating various child materialized views. Data extraction queries select the best MV which can fulfill its data requirements. For creating child MVs, initially the data types of fields/columns of the base MV are determined. All of the columns are grouped according to the data types. In case of numeric data types, those columns are separated which cannot be aggregated e.g, ID, SSN, from numeric attributes where various aggregation operations can be carried out. This whole process is carried out for string attributes as well. This whole process result into an aggregation plan, which later on is translated into a script and is then executed. The process of query answering is made efficient by having more MVs having the potential data required to fulfill maximum requirements of query.

In this paper [10], author had designed and developed SPARSE on android based mobile phone to authenticate securely using Bluetooth on Remote system. Further they had evaluated cryptographic operations of IBE scheme. This scheme can be further explored to implement on different platforms and Key revocation problems can be explored in future. The implementation needs thorough security analysis to be carried out.

In this paper [11] authors states that Magnus Kallus encryption scheme has tremendous potential, it can be combined with other encryption schemes such as RSA, DES, Diffie-Hellman Key Exchange, to make a new scheme for encryption. It may further be implemented for Digital Signatures. Other protocols can also be used for security of the keys like Diffie-Hellman Key Exchange or use a random number algorithm for generating the random numbers.

In this paper [12] author has explained that some of the existing transposition techniques for creating a cipher text corresponding to the given plain text. Author has also given new technique for the encryption and decryption process is tested rigorously on different cases and verified results and found to be very correct and is working properly and it is able to encrypt and decrypt the plain text in the form of alphanumeric character, symbols, or any ASCII character without any loss of information and maintain the security of the message during the transmission over the network. Author has also determined that after preordering process for a 15 character size we can get it by 9 steps of preordering process (as 4 times in encryption process and 5 times in decryption process), the original data that was before preordering process.

In this paper [13] author proposed a scheme according to the challenging issues during the user authentication and access control process in cloud-based environments, an efficient and scalable user authentication. In the proposed scheme client-based user authentication agent was introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a service application was used to confirm the process of authentication for un-registered devices.

In the proposed scheme two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers. In

overall, the theoretical analysis of the suggested scheme shows that, designing this user authentication and access control model will enhance the reliability and rate of trust in cloud computing environments as an emerging and powerful technology in various industries.

3. Conclusion

In this paper, we discussed various techniques that are used as pre-calculate methods and we had also discussed the techniques for authentication. Storing data in the cloud storage is based on various algorithms. There are various technologies that have been implemented for increasing the performance of accessing stored data in the cloud but they are not efficient. Although there are various authentication schemes have been implemented for the security of these data but either they are too much complex or they require huge network resources.

In most of the papers conventional password authentication schemes is used where server maintains password table or verification table which contains user identifier (ID) and password (PW) for all the registered users. It is used to authenticate the legitimate user. Short surveys of various pre-calculate techniques and security authentication has been given.

Reference

[1] J. Junkawitsch, L. Neubauer, H. Höge, and G. Ruske presented paper entitled "A New Keyword Spotting Algorithm With Pre-Calculated Optimal Thresholds" IEEE ON Spoken Language, 1996. ICSLP 96.

[2] M. Sobotka, D. Wollherr, M. Buss presented paper entitled "A Jacobian Method for Online Modification of Precalculated Gait Trajectories" at 6th International Conference on Climbing and Walking Robots CLAWAR2003 Catania, Italy, pp. 435.442, 2003.

[3] Marek Gayer and Pavel Slavík presented paper entitled "Pre-Calculated Fluid Simulator States Tree" at OACTA Prees Proceeding (410) Applied Simulation and Modelling – 2003.

[4] Dmitriy Kuptsov, Andrey Khurri, and Andrei Gurtov presented paper entitled "Distributed User Authentication in Wireless LANs" at IEEE in 2009.

[5] Chia-Sheng Tsai and Cheng-I Hung presented paper entitled "An Enhanced Secure Mechanism of Access Control" at IEEE in 2010.

[6] Sridhar S and Vimala Devi.K presented paper entitled "Nested Mechanism for Mutual Authentication" at IEEE in 2011.

[7] Yanan Sun, Xiaohong Guan, Ting Liu and Yu Qu presented paper entitled "An Identity Authentication Mechanism Based on Timing Covert Channel" at 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[8] Liu Yang, Rongrong Ni, Yao Zhao presented paper entitled "Segmentation-based Image Authentication and Recovery Scheme Using Reference Sharing Mechanism" at 2012 International Conference on Industrial Control and Electronics Engineering.

[9] Muhammad Saqib, Muhammad Arshad, Mumtaz Ali, Nafees Ur Rehman and Zahid Ullah presented paper entitled "Improve Data Warehouse Performance by Preprocessing and Avoidance of Complex Resource Intensive Calculations" at International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[10] Shivraj V L, Rajan M A and Balamuralidhar P presented paper entitled "Secure Personal Authentication through Remote System for E- Transactions (SPARSE)" at IEEE in 2014.

[11] Vipul Srivastav presented paper entitled "New Approach in Encryption: Magnus Kallus" at IEEE 2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[12] Nikhil Agrawal, Manoj Kumar and Dr. M.A. Rizvi presented paper entitled "Transposition Cryptography Algorithm using Tree Data Structure" at IEEE ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India.

[13] Faraz Fatemi Moghaddam, Shiva Gerayeli Moghaddam, Sohrab Rouzbeh, Sagheb Kohpayeh Araghi, Nima Morad Alibeigi and Shirin Dabbaghi Varnosfaderani presented paper entitled "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments" at 2014 IEEE Region 10 Symposium.

[14] Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011.