iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** III **Month of publication:** March 2018

DOI: http://doi.org/10.22214/ijraset.2018.3468

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Security and Efficiency of Content-Centric Networking

Dhanalakshmi.G[1], Deepak.S[2], Jeffrey Shadrach.S[3], Jude Farrington.S[4]
[1]*Associate Professor,* [2-4] *Ug Scholar, Department of Information Technology, Panimalar Institute of Technology Chennai, India*

Abstract: ***Information-Centric Networking (ICN) is an emerging networking paradigm where named and routable data (content) is the focal point. Users send explicit requests (interests) which specify content by name, and the network handles routing these interests to some entity capable of satisfying them with the appropriate data response (producer). One key feature of ICN is opportunistic in-network content caching. This property facilitates efficient content distribution by reducing bandwidth consumption, lessening network congestion, and improving the content retrieval latency by users (consumers). Unfortunately, the same feature is also detrimental to privacy of content consumers and producers. Simple to implement, and difficult to detect, timing attacks can exploit ICN routers as "oracles" and allow an adversary to learn whether a nearby consumer recently requested certain content. The attack leverages a timing side channel that relies on router caches and is implemented by requesting a few packets from each piece of content being probed. Similarly, probing attacks that target content producers can be used todiscover whether certain content has been recently distributed. After analyzing the scope and feasibility of such attacks, we propose and evaluate some efficient counter measures that offer quantifiable privacy guarantees while retaining the benefits of ICN.***

Keywords: Time Scheduling, Privacy aware caching, First in first out.

I. INTRODUCTION

As the increasing number of smart devices and various applications, IT services have been playing an important role in our daily life. In recent years, the quality and resilience of services have been drawing increasing attention. For example, it is important to optimize the delay.

Information-Centric Networking (ICN) is an emerging networking paradigm where named and routable data (content) is the focal point. ICN is opportunistic in-network content caching, facilitates efficient content distribution by reducing bandwidth consumption, lessening network congestion, and improving the content retrieval latency by users (consumersThe goal of CCN is to provide more flexible and scalable network there by addressing the Internet's modern-day requirement .The CCN is characterized by the excange of content request messages and content returns messages. When requested by name,CCN deleivers named content to the user front he nearest cache,traversing fewer network hops,eliminating redundant requests and consuming less resourses overall. But the same feature also provides privacy issues on the consumers data and it is difficult to detect the issue.ICN is simple to implement Moreover, when multiple request occur at the same time, we need an intelligent scheduler to determine which request to process first or which ones can be done simultaneously, in order to minimize the total time taken.this is done by the time scheduling algorithm. We also implement Privacy aware caching algorithm to prevent from further hacking of the database.

II. RELATED WORKS

Title : Outsourced Symmetric Private Information Retrieval
Author : Stanislaw Jarecki
Year : 2014

In the setting of searchable symmetric encryption (SSE), a data owner D outsources a database (or document/file col- lection) to a remote server E in encrypted form such that D can later search the collection at E while hiding information about the database and queries from E. Leakage to E is to be confined to well-defined forms of data-access and query patterns while preventing disclosure of explicit data and query plaintext values. Recently, Cash et al. presented a protocol, OXT, which can run arbitrary boolean queries in the SSE setting and which is remarkably efficient even for very large databases.

Title : Scalable Verification for Outsourced Dynamic Databases
Author : HweeHwa Pang,
Year :2007

A. Description

Query answers from servers operated by third parties need to be verified, as the third parties may not be trusted or their servers may be compromised. Most of the existing authentication methods construct validity proofs based on the Merkle hash tree (MHT). The MHT, however, imposes severe concurrency constraints that slow down data updates. We introduce a protocol, built upon signature aggregation, for checking the authenticity, completeness and freshness of query answers. The protocol offers the important property of allowing new data to be disseminated immediately, while ensuring that outdated values beyond a pre-set age can be detected. We also propose an efficient verification technique for ad-hoc equijoins, for which no practical solution existed. In addition, for servers that need to process heavy query workloads, we introduce a mechanism that significantly reduces the proof construction time by caching just a small number of strategically chosen aggregate signatures. The efficiency and efficacy of our proposed mechanisms are confirmed through extensive experiments.

Title : Dynamic Searchable Encryption via Blind Storage
Author : Muhammad Naveed
Year : 2001
Description:
Dynamic Searchable Symmetric Encryption allows a client to store a dynamic collection of encrypted documents with a server, and later quickly carry out keyword searches on these encrypted documents, while revealing minimal information to the server. In this paper we present a new dynamic SSE scheme that is simpler and more efficient than existing schemes while revealing less information to the server than prior schemes, achieving fully adaptive security against honest but curious servers.

Title : Publicly Verifiable Conjunctive Keyword Search in Outsourced Databases
author: Monir Azraoui
Year : 2015.
Description:
Recent technological developments in cloud computing and the ensuing commercial appeal have encouraged companies and individuals to outsource their storage and computations to powerful cloud servers. However, the challenge when outsourcing data and computation is to ensure that the cloud servers comply with their advertised policies. In this paper, we focus in particular on the scenario where a data owner wishes to (i) outsource its public database to a cloud server; (ii) enable anyone to submit multi-keyword search queries to the outsourced database; and (iii) ensure that anyone can verify the correctness of the server's responses. To meet these requirements, we propose a solution that builds upon the well-established techniques of Cuckoo hashing, polynomial-based accumulators and Merkle trees. The key idea is to (i) build an efficient index for the keywords in the database using Cuckoo hashing; (ii) authenticate the resulting index using polynomial-based accumulators and Merkle tree; (iii) and finally, use the root of the Merkle tree to verify the correctness of the server's responses. Thus, the proposed solution yields efficient search and verification and incurs a constant storage at the data owner. Furthermore, we show that it is sound under the strong bilinear Diffie-Hellman assumption and the security of Merkle trees..

B. Problem Statement

The user logs on to the system with the help of the user name and password by simple registration process providing user name and password. After successful login the user can access all the file hence providing less security and there is no admin to watch the login details details of the user.

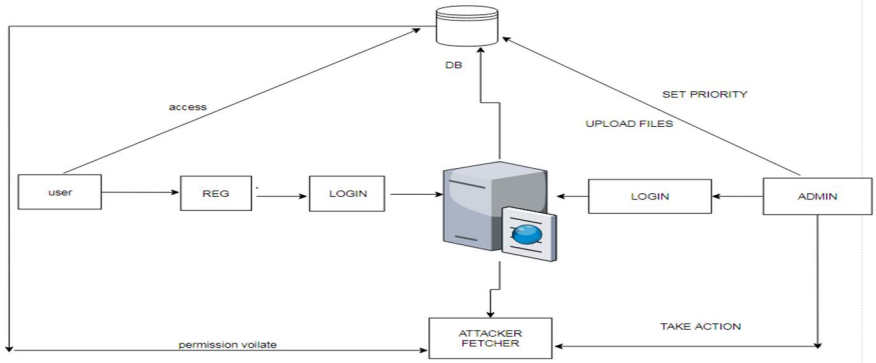
C. Disadvantages

1) It is not effective.
2) Security is very less.

III. PROPOSED SYSTEM

First-in, First-out (FIFO): Evict the page that has been in the cache thelongest.
Time Scheduling Algorithm: Time is been scheduled and allocated for theusers at which time they can access the server .
Security is one of the most challenging ongoing research area in Server computing because data owner stores their sensitive data to remote servers and users also access required data from remote servers which is not controlled and managed by data owners. In this proposed System, a PASA (Privacy-Aware Security Algorithm) for Server environment which includes the three different security schemes to achieve the objective of maximizing the data owners control in managing the privacy mechanisms.

A. Architectural Diagram



IV. MODULES USED

A. User Interface

This is the second module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

B. File Upload

In his module, the admin process is to move into file upload window to upload file. The admin process is to upload the files. Data owner uploads the file in cloud storage for user's view. While uploading the file the admin generates the key for security purpose and uploads into cloud.

C. File Name Sharing

In this third Module the project will view the uploaded files list in my project for confirmation and analysis use. If the process of the fully analysis by the user and the fully uploaded data. In this finally request the wanted own file from the uploaded file.

D. Time Schedule request and request

This is the fourth module of our project. The important role for the admin is to move login window to user requested window. This module has created for the user friendly purpose. In this login page we have to enter login user id and password. It will check username and schedule time is match file will be download. If we enter any invalid usename or invalid schedule time we can't enter into download it will shows error message. So we are preventing from unauthorized people entering access. It will provide a good user friendly for our project. It will reduce the server breakdown. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

E. User File Download

This is the third module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, the data user request for the file access from the admin where the admin handles the file access key and providing the key to the authorized user. if the user want to change the key then user have to send revocation request.

V. TECHNOLOGIES USED

A. MVC (Model, View, Controller)

MVC stands for Model View and Controller. It is a design pattern that separates the business logic, presentation logic and data. Controller acts as an interface between View and Model. Controller intercepts all the incoming requests. Model represents the state of the application i.e. data. It can also have business logic. View represents the presentation i.e. UI (User Interface).

B. JSP

In our project we are using Jsp to design the application process. JSP pages are using to develop the form pages like login and user registration pages. It means it is mainly useful for user Interaction development. And some static content of html pages to jsp pages for dynamic content.

C. Servlet

In our project we are using Servlet to control the application process. Servlet is the center of our application because all the controlling part will be monitoring by the Servlet only. It means Servlet takes requests and matches for suitable jsp's and it is also useful for database controlling.

D. INTERFACES

An interface is a collection of abstract methods. A class implements an interface, thereby inheriting the abstract methods of the interface.An interface is not a class. Writing an interface is similar to writing a class, but they are two different concepts. A class describes the attributes and behaviors of an object. An interface contains behaviors that a class implements

E. Bean Classes

In our project we are using Java Beans;JavaBeans are reusable software components for Java. They are classes that encapsulate many objects into a single object (the bean). They are serializable, have a 0-argument constructor, and allowaccess to properties using getter and setter methods.

F. Java Script

JavaScript is a dynamic computer programming language. It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages. In this project we are using JavaScript validation purpose.

G. Jdbc

JDBC is a Java database connectivity technology (Java Standard Edition platform) from Oracle Corporation. This technology is an API for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database.

VI. ACKNOWLEDGEMENT

We thank our Head of the Department (IT) Dr. A. Joshi for providing us all the necessary facilities. We express our sincere thankfulness to our Project Guide Mrs. Dhanalakshmi. G for her successful guidance to our project. Without the help it would be a tough job for us to accomplish this task. We thank our guide for her consistent guidance, encouragement and motivation throughout our period of work.

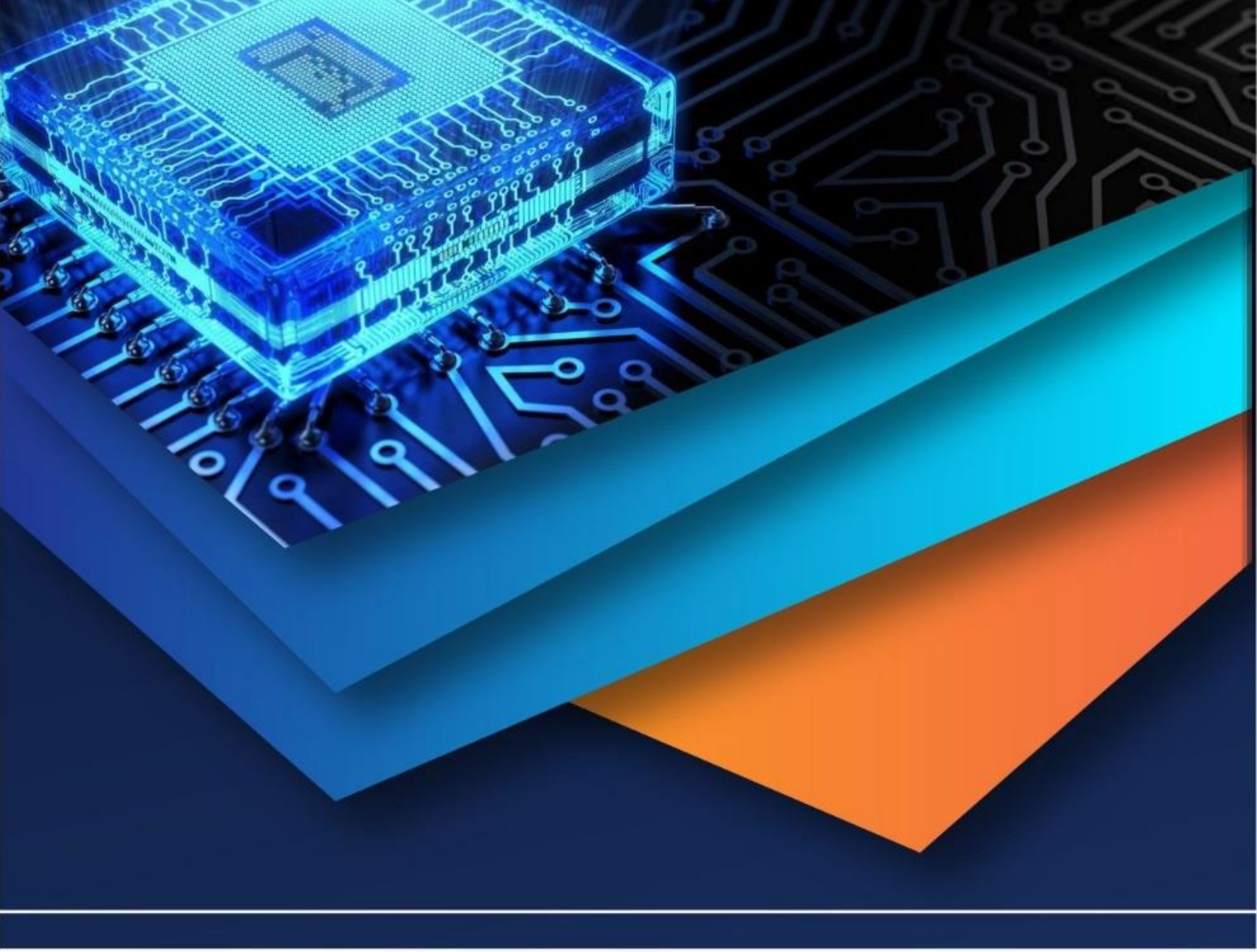
VII. CONCLUSION

As a result the schemes are used to achieve the objective of maximizing the data owners control in managing the privacy mechanisms . Introduction of formal model that allows us to quantify the degree of privacy offered by algorithms. The security is high and very effective in nature with the privacy mechanisms.

REFERENCES

[1] S. Jiang, X. Zhu, L. Guo, and J. Liu, "Publicly verifiable boolean query over outsourced encrypted data," in Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015.
[2] S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Outsourced symmetric private information retrieval," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. ACM, 2013, pp. 875–888.
[3] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 965–976.
[4] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in Advances in Cryptology- CRYPTO 2013. Springer, 2013, pp. 353–373.
[5] M. Naveed, M. Prabhakaran, and C. A. Gunter, "Dynamic searchable encryption via blind storage." in Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, May, 2014.

[6] E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic searchable encryption with small leakage." IACR Cryptology ePrint Archive, vol. 2013, p. 832, 2013.
[7] D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M. C. Rosu, and M. Steiner, "Dynamic searchable encryption in verylarge databases: Data structures and implementation," in 21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014, 2014.
[8] S. Faber, S. Jarecki, H. Krawczyk, Q. Nguyen, M. Rosu, and M. Steiner, "Rich queries on encrypted data: Beyond exact matches," in European Symposium on Research in Computer Security (ESORICS 2015). Springer, 2015, pp. 123–145
[9] M. Azraoui, K. Elkhiyaoui, M. Onen, and R. Molva, "Publicly verifiable conjunctive keyword search in outsourced databases," in Proceedings of the 2015 IEEE conference on Communications and Network Security (CNS). IEEE, 2015, pp. 619–627.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY