S

skm

User Name:	skm
Job Name:	85
Host Name:	dagonet.cs.purdue.edu
Printer Name:	bradley
Date:	05/04/2000 11:44:24 AM

S

skm

User Profile Driven Web Security

Sanjay Madria, Mukesh Mohania
Bharat Bhargava
Department of Computer Science
Purdue University, West Lafayette
skm, bb@cs.purdue.edu

- Security over the web is one of the major issues concerning data sharing over clients and servers.
- Many organizations are keeping their company data on the web, it is important to protect information fully/partially from the unauthorized users.

- Every server on the internet is susceptible to security risks in at least one of the following ways:
- -Unauthorized users access information that they are not supposed to access
- -Unauthorized users replacing original contents with unreliable or unwanted information on web pages
- Restricted access to web database through CGI/JDBC/ODBC

- The distribution and sharing of web information that must be accessed in a selective way requires the enforcement of security controls, ensuring that information will be accessible only to authorized entities.

Current Access Control Methods

- User based restriction: (username, password) is required to access information ;It has either all or none property
- Domain restriction: Web allows for access to resources to be restricted by domain (.com); Internet Service Provider (ISP) would not have a “.com” domain associated with the connections.
- Browser based methods (embedded Secure Socket Layer)

Examples

- Credit history verification
- Students grades sharing
- Targeting potential customers
- Providing information at multiple granularity for security concerns

Disadvantages

- System has to maintain either a pre-defined set of user names or a pre-defined set of domain names or both, and access restrictions for each.
- It is very restrict and not very flexible

Our Objective

- How to Protect web information and at the same time allow partial information to be visible
- How to provide access to different users so that different users can have different view of data (some details can be hidden for security reasons)
  - Low quality of data
  - control on the abusive language
  - different resolution of images

Security Methods

- Static Level Security: for predefined users and domain
  - Virtual web view: computed dynamically on demand
  - Materialized web views: pre-computed and stored in Web warehouse
  - ‘Query driven’ method

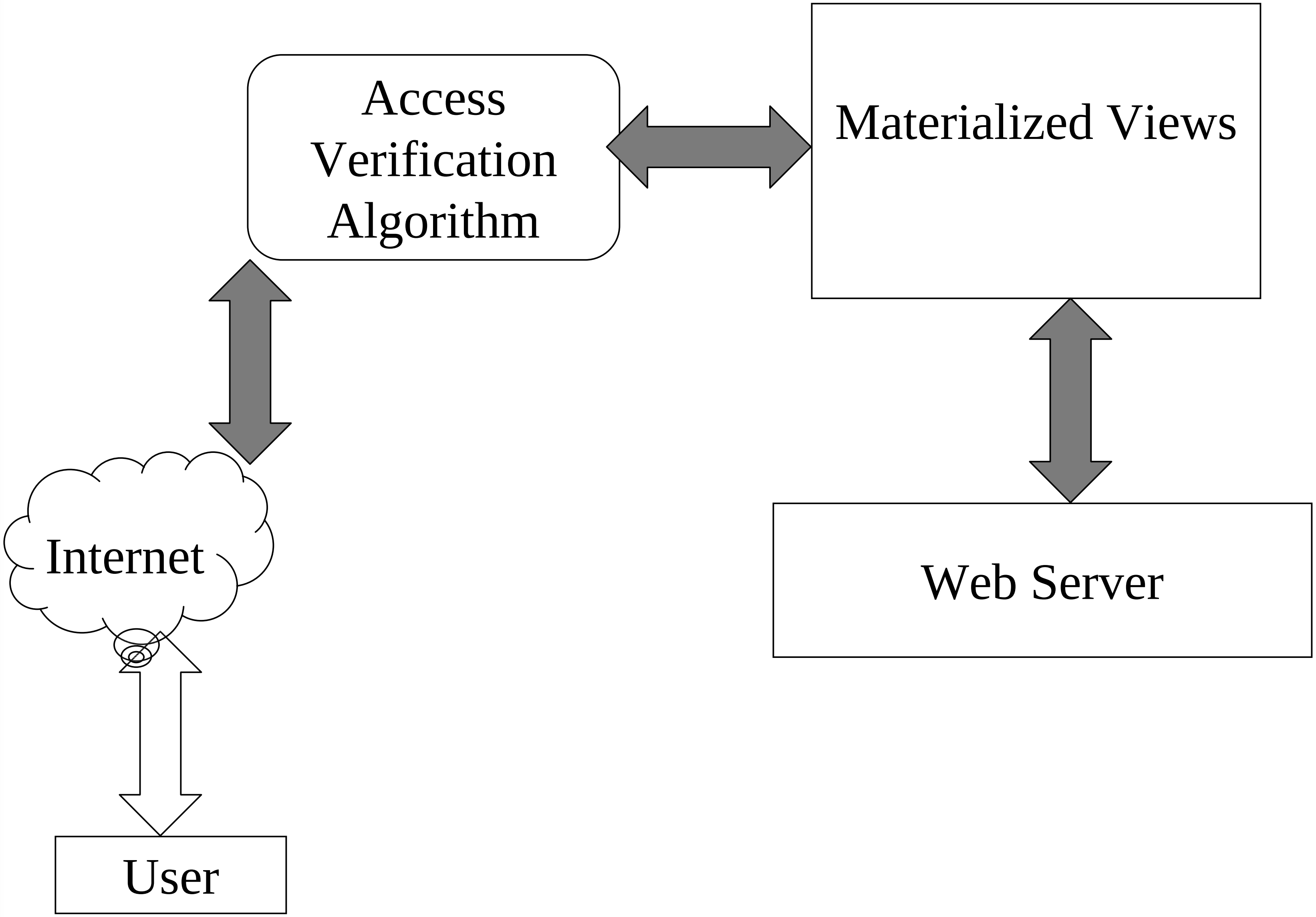
Open Problems

- how to build user profiles and represent them
  - – include past behaviour
  - – relevance feedback
  - – earlier queries
  - – set of important keywords
  - – type, content and duration
- How to divide user into different levels based on user profile
- how to authenticate users input
-

– Extend XML or HTML to provide security at ‘tag’ level and define whether a user can access that tag or not.

– Define various levels of security for different types of users

– Provide different view of the same data for security reasons



Access Verification Algorithm

Materialized Views

Internet

Web Server

User

Dynamic Level Security

- Static level security restricts information sharing.
- An agent interacts with the user cumulatively and provides authentication and personalized views based on analysis and verification of the interactive results.
- Views are created on the fly based on verification and system dependent reasons.

Problems

- To perform a user interaction session
  - It can be done with the help of mobile agent
- To verify the data provided by the user is valid and to define a method to identify the right users
  – it involves analysis of the user input.

- To determine a method to decide on access privileges given to the user.
  - Upon determination of the user’s validity, the agent creates a session id for the user, and assigns access permission to the data that resides on the server.

Solution

- User profiles are used for providing different levels of security
- Each user can have a profile stored at the web server or at third party server
- User can change profile attributes at run time
- User behavior is also taken into account based on past record
- Agent access the web page on behalf of the user and try to negotiate with web server for the security level

User Profile

- Personal category
  - personal identifications ; name, dob, ss etc.
- Data category
  - Document content ; keywords
  - document structure; audio/video, links
  - source of data
- Delivery data - web views, e-mail
- Secure Data Category
  - Personal data may be secured