GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

MITIGATION OF INSIDER DATA THEFT ATTACKS USING FOG COMPUTING

A Report for the Evaluation 3 of Project 2

Submitted by

Abhinav Anand

16SCSE101283

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE ENGINEERING

COMPUTING SCIENCE & ENGINEERING

Under the Supervision of

Prof G.Nagarajan

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

20 MAY 2020

GALGOTIAS UNIVERSITY

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

SCHOOL OF COMPUTING SCIENCE & ENGINEERING

BONAFIDE CERTIFICATE

Certified that this project report "**.MITIGATION OF INSIDER DATA THEFT ATTACKS USING FOG COMPUTING"** is the bonafide work of "**Abhinav Anand"** who carried out the project work under my supervision.

Signature of the	Signature of the
Head of department	of the supervisior
SIGNATURE	**SIGNATURE**

Acknowledgement

A journey is easier when we travel together. Interdependence is certainly more valuable than independence. This dissertation is the result of work whereby I have been accompanied and supported by many people. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

I express my sincere gratitude to my guide **Prof. G.Nagarajan** for his constant guidance, encouragement and inspiration throughout the project work. His interest and confidence in me was the reason for all the success I have made. I have been fortunate to have him as my guide as he has been a great influence on me, both as a person and as a professional.

I would also like to thank my Head of Department , Project Coordinator and all the faculty members of the department of computer science for their valuable suggestions and helpful discussions.

I would like to thank all my friends for their smiles and friendship, making the life at Galgotias University enjoyable and memorable.

Above all, I am blessed with such caring parents. I extend my deepest gratitude to my parents and my elder sisters for their invaluable love, affection, encouragement and support.

ABHINAV ANAND

Abstract

Fog computing is currently daily in favor of all sorts of business units. We can access and store all types of application and data in Fog. As it comes up with a lot of facilities, it becomes exhausting to entrust security. Fog computing provides different security approaches than conventional slant like cryptography. By observing actions and reactions of user whereas accessing the info, we will realize the abnormal behavior. If unauthorized access detected even after prying difficult queries verification, then we can introduce disinformation attack and provide the fake worthless information to attacker. It will be useful to regulate effectiveness of data. Experiments done by author, shows that, this method might give extraordinary level of security for knowledge in Fog computing atmosphere. Fog computing is preventive disinformation attack

List of Figures

List of Tables

List of Keywords

AES = Advanced Encryption System

MAC = Media Access Control

IP = Internet Protocol

CHAPTER I

Introduction

Traditional business needs a data centre, complex software's and a team of experts to run them. So Fog computing becomes more and more popular because of its flexibility, cost effectiveness, easy deployment. The Fog Security Alliance (2009) declares that the “Fog describes the utilization of a group of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. As Fog computing offers such a large amount of advantages to businesses, its security and trustworthiness has always been in question. Security is a very vital demand for any IT application, as nobody wants their data to be accessed by unauthorized users. There are many Fog security methods available for external threats. The methods available for external attack have not been able to prevent data theft. Van Dijk and Juels have shown that the solutions like encryption and decryption are not sufficient data protection mechanism when used alone by using fully homomorphism encryption. The ability to leave no trace of an attack is the biggest security challenge for this Fog environment. The lack of resources and evidence makes it difficult to find Fog -based cyber attacks. Data theft attack detection is very difficult when attacker is insider. According to the 2011 Cyber Security Watch Survey conducted on 607 businesses, government executives, professionals and consultants, 21% of cyber-attacks were caused by insiders. 33% of the respondents thought the corporate executive attacks were a lot of expensive and damaging to organizations Insiders may get the credentials of authorized user of by password sniffing or key logger etc for accessing system or network. Rocha and Correia show that it's terribly simple to steal passwords for a malicious corporate executive of the Fog service provider .Another case can be like insider may attack on system by taking advantage of victim’s unwise trust like person leaves terminal open or permitting to use terminal to workfellow are often create as masquerade attack. So that service provider cannot get plan of Associate in nursing attack on the system as a result of offender has identity of licensed user. The most common method wont to observe masquerade attack is to stay record of user behavior and to search out abnormal behaviour. In this approach, user’s actions are profiled to form a baseline of normal behaviors. Salvatore J. Stolfo and Malek Ben Salem proposed a unique approach to secure Fog by mistreatment decoy info technology that they known as as Fog Computing.

This technique can use the MAC , IP address, Time Slot and AES formula. The MAC address improves the chances of identifying attacks details, AES algorithm will encrypt the requested Password by the User. And Time Slot Use for attacker Attacks the Data.

Problem Statement

We propose a different approach for securing data in the server using offensive decoy technology. We monitor data access in the Fog and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a server environment. We propose a completely different approach to securing the server using decoy information technology, that we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.

Research Objective

Breach of security happens from outside of the organizations additionally as from at intervals. Consistent with Cyber Security Watch Survey conducted in 2017 on 700 professionals, businesses, consultants and government executive's insiders are chargeable for 22% of the total cyber-attacks.34% of the respondents contemplated that the attacks by the insider were additional expensive and damaging to organizations. The foremost common within attacks are unauthorized access to and use of company data (64%), unplanned revealing of personal or sensitive information (58%), virus, worms, or alternative malicious codes (38%), and larceny of belongings (34%). The Fog computing vulnerabilities to malevolent corporate executive are: inexact roles and responsibilities, poor social control of role definitions, non pertinences of need-to-know principle, vulnerabilities, system or OS vulnerabilities, and scant physical security procedures, unusefulness of process information in encrypted kind, application vulnerabilities or poor patch management.

Malicious disruption of an organization’s sensitive data resources might lay the complete victim organization’s operation on the road. There are three kinds of Fog -related corporate executive threats: the villain administrator, insiders who exploit Fog vulnerabilities, and also the insiders who use the Fog to conduct infamous activity. Villain administrator has privilege to steal unprotected cases, brute-force hit over passwords, and transfer customers’ information from the casualty organization. Insiders who utilize Fog vulnerabilities try to gain unauthorized access to confidential information in an organization; they may create a fortune by merchandising the sensitive data, or use the data for his or her future businesses.

Significance of Study

Data discharge happens daily wherever guidance like user information, ASCII text file or style specification, price hits, material possession, trade secrets, etc. are leaked out. When these are leaked it leaves the company unprotected and goes outside the jurisdiction of the cooperation. This uncontrolled data puts business in a vulnerable position.

Once this information isn't any longer inside the domain, then the corporate is at serious risk. This research seeks to help detect leakage and sensitive data in a cloud environment because when cybercriminals, for instance, sell this data for profit, it cost organizations money, damages

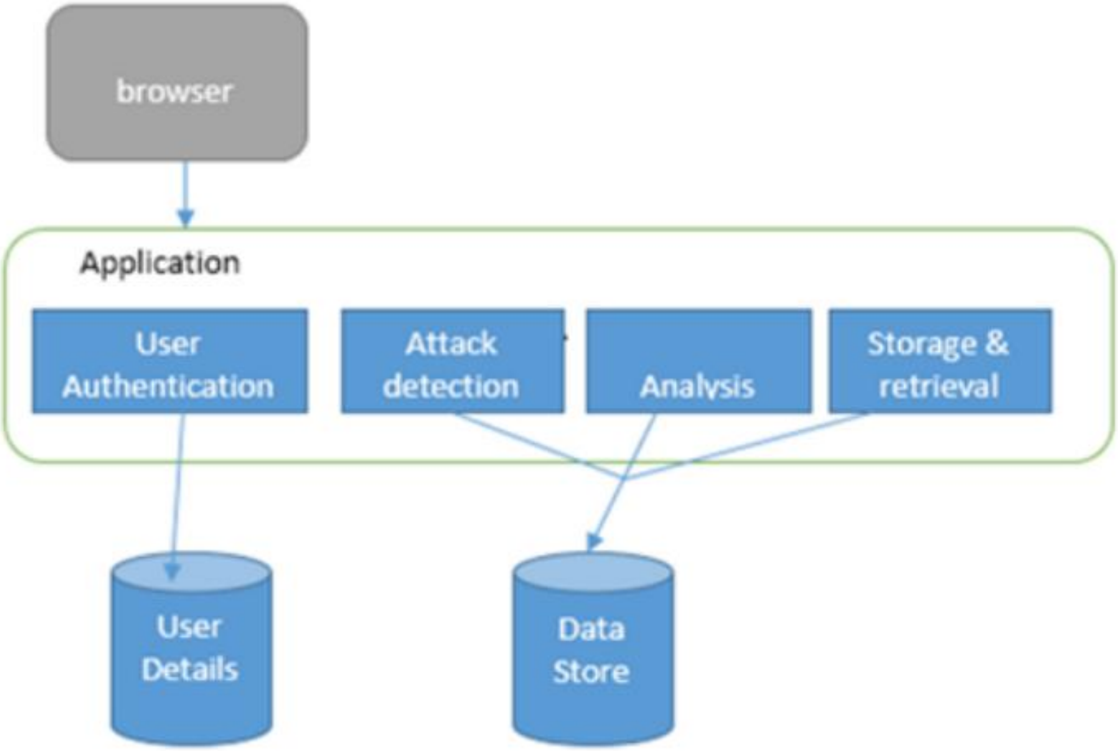


Figure 2.0 System Architecture

Scope of the Research

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

- Our goal is to detect when the distributor's sensitive data has been theft by Attack, and if possible to identify the Attacker that Attack the data.
- Perturbation is a very useful, technique where the data is modified and made "less sensitive" before being handed to User.
- We develop unobtrusive techniques for sleuthing theft of data.
- We also present, algorithms for distributing objects to agents, in a way that improves our chances of identifying a Attacker.
- Finally, we also consider the option of adding "fake" data to the Attacker set. Such objects don't correspond to real entities however seem realistic to the user
- When Data theft by Attacker Send Email to User with MAC Address.

CHAPTER II

LITERATURE REVIEW

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

AES (ADVANCED ENCRYPTION STANDARD) ALGORITHM

AES (Advanced Encryption Standard) algorithm is a symmetric block cipher. It is best algorithm for security purpose. AES does not uses a fiestel structure. Instead, each full round consist of four separate functions: Byte substitution, Permutation, Arithmetic operation and XOR with a key. It uses 128 bit for block size and 128, 192 or 256 bits for key size. , Four different stages are used: One of Permutation and other three for Substitution.

 Substitution byte: Uses an S-box to perform byte-by-byte substitution of the blocks.

 Shift rows: A simple permutation. Mix Columns: A substitution that makes use of arithmetic over GF

 Add Round key: A simple bitwise XOR of the current block with a portion of the expanded key.

This new encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century,- according to the NIST announcement of the process for development of an advanced encryption standard algorithm. It was intended to be easy to implement in hardware and software, as well as in restricted environments and offer good defenses against various attack techniques.

AES features

The selection process for this new symmetric key algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs fulfill submitted.

NIST specified the new advanced encryption standard algorithm must be a block cipher capable of handling 128 bit blocks, using keys sized at 128, 192, and 256 bits. Other criteria for being chosen as the next advanced encryption standard algorithm included :

Security- Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.

Cost- Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

Implementation- Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

How AES encryption works

AES contains 3 block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts information in blocks of 128 bits victimization crypto logic keys of 128-, 192- and 256-bits, severally. The Rijndael cipher was designed to simply accept extra block sizes and key lengths, except for AES, those functions weren't adopted.

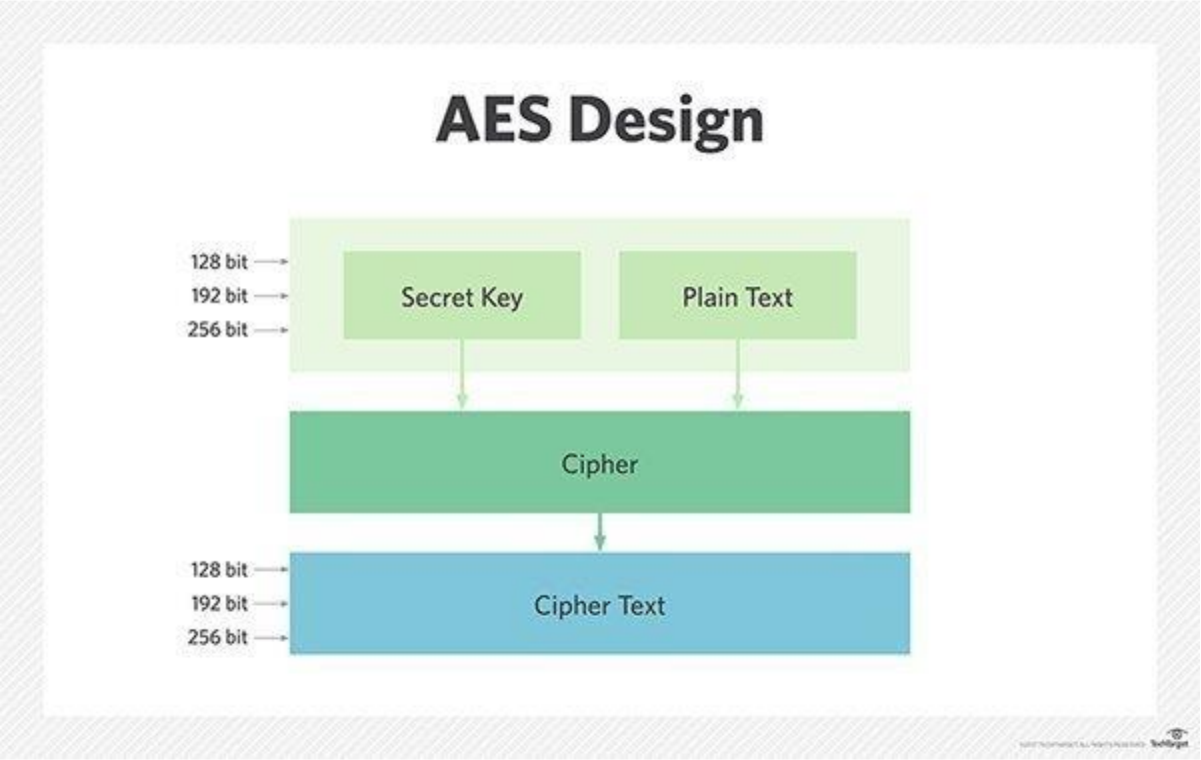


Figure 2.1: AES Design.

Symmetric (also called secret-key) ciphers use a similar key for encrypting and decrypting, therefore the sender and therefore the receiver should each understand -- and use -- a similar secret key.

All key lengths square measure deemed sufficient to shield classified info up to the "Secret" level with "Top Secret" info requiring either 192- or 256-bit key lengths.

There square measure ten rounds for 128-bit keys, twelve sphericals for 192-bit keys and fourteen rounds for 256-bit keys -- a round consists of many process steps that embrace substitution, transposition and mixture of the input plaintext and remodel it into the ultimate output of cipher text.

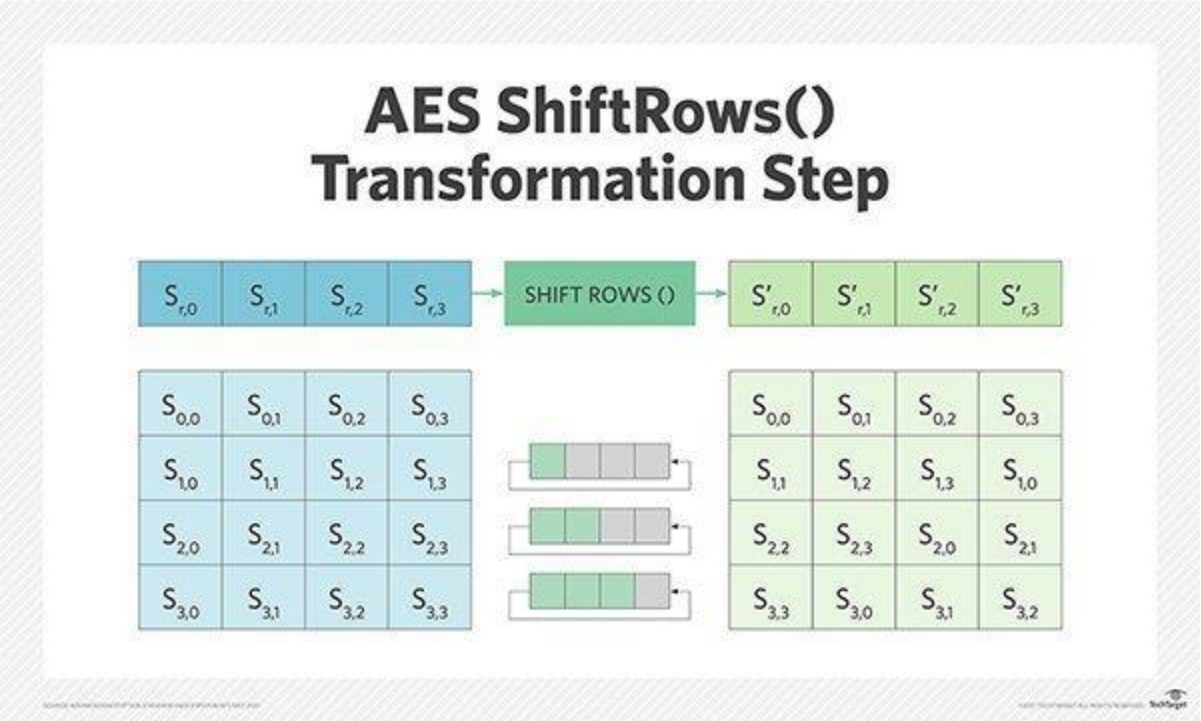
The AES cryptography formula defines variety of transformations that square measure to be performed on knowledge keep in associate array.

The first step of the cipher is to place the information into associate array; once that the cipher transformations square measure continual over variety of cryptography rounds.

The number of rounds is decided by the key length, with ten rounds for 128-bit keys, twelve rounds for 192-bit keys and fourteen rounds for 256-bit keys.

The first transformation within the AES cryptography cipher is substitution (of knowledge of knowledge of information) employing a substitution table; the second transformation shifts data rows, the third mixes columns.

The last transformation is a simple exclusive or (XOR) operation performed on each column using a different part of the encryption key -- longer keys need more rounds to complete.


AES ShiftRows()
Transformation Step
$S_{r,0}$ $S_{r,1}$ $S_{r,2}$ $S_{r,3}$
SHIFT ROWS ()
$S'_{r,0}$ $S'_{r,1}$ $S'_{r,2}$ $S'_{r,3}$
TechTarget

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

Figure 2.2 AES Shift Rows() Transformation Step

MAC (MEDIA ACCESS CONTROL)

A Mac (Media Access Control) could be a distinctive symbol allotted to network interfaces for communications on the physical network phase. Each and every computer has a unique MAC address for its Ethernet, Modem , Wireless network card.

Each and every network devices have a novel completely different MAC address. Mac address contains numbers and letters. Numbers from zero to nine and letters from A to F.

For demonstration : 00:0E:84:27:3D:E7.

In this system Mac address is employed for detection the guilty agent.

If agents Mac address pair with hold on Mac address then it'll be a guilty agent.

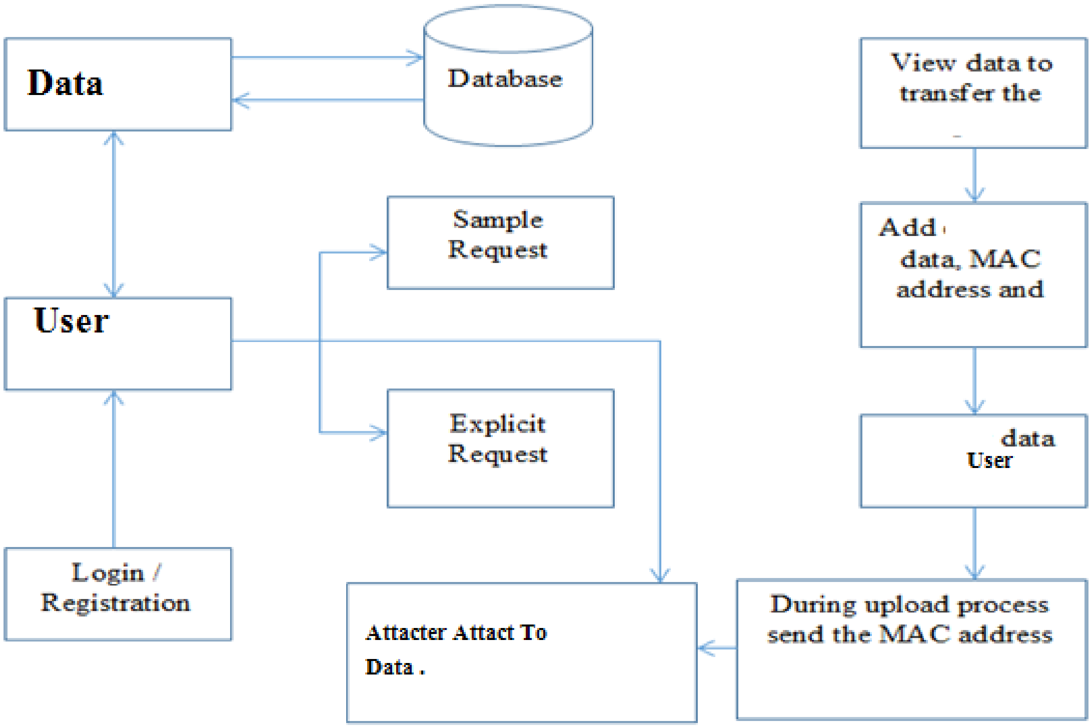


Figure 2.3 Fog Computing Defense from Security Threats Cyber Attacks and Prevention.

Step 1: The authorized User should fill the registration form. The registration form has all the information about the User. And Security Question , Time Slot ,Automatic Generate Key when it submits the form, receipt on your user mail with Generate Key System.

Step 2: User Login with Valid User name and password And Upload data from pc to cloud after User View All data or specific Data in Your Webpage Screen.

Step 3: When User want Download Data, During document access, the user key specified is tracked along with the type of operation i.e., valid or invalid, if invalid MAC address, Mail to user mail ID.

Step 4: Only authorized user is able to Store Data on the server side by checking the Attacker MAC address with stored MAC address. It will also check the authority of the user before data.

Step 5: The unauthorized User (Attacker) is unable to download the data.

Step 6: If an Attacker wants to use the data, it should upload data. Upload data contains. And before uploading data on the server side, the system checks the MAC address of the agent. If the MAC address is different than it identifies a Attacker.

Step 7: So, from this system improve the chances of identifying an attacker.

Cloud Computing

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It is divided into three type :

1. Application as a service.

2. Infrastructure as a service.

3. Platform as a service.

Cloud computing exhibits the following key characteristics:

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

2. **Cost** is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower 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.

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.

3. Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

4. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

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

6. Utilization and efficiency improvements for systems that are often only 10-20% utilized

7. **Reliability** is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

8.Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

9. Security could 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. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being 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.

10. 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.

Decoy documents

We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. We launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user’s real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:

(1) Validating whether data access is authorized when abnormal information access is detected, and

(2) Confusing the attacker with bogus information..

Security Management

- ✓ It reveals defense organization frameworks by as well as standards which are essential for the cloud. With the implementation of cloud computing services (public, private and hybrid or partner), a large part of a customer’s network, system, applications, and data move under third-party provider control.

- ✓ The services delivery model creates cloud of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud CSP. This shared responsibility model brings new security management challenges to the organization’s Information Technology operations staff.

- ✓ Adequate transparency from cloud services to manage the governance - the implementation of security management processes to assure the business that the data in the cloud is appropriately protected through properly configured identity and access management tools must be ensured.

CHAPTER III

METHODOLOGY

The main point of the learn is to show how user accessibility and activity to a computing resource could be tracked, monitored and audited to protect the integrity, ease of use and availability of data to certified and authenticated users in cloud application. The strategy was to adopt Any Software as a case study. This is because these hospital software hosted in cloud environments have no local databases, different access levels and remote user authentications and authorization.

3.1.2 Instrumentations

A prearranged non - disguised depth discussion was conducted and address the subsequent functions. Nature of working environment users involved and the type of use self and authorization system in place and finally audit sprawling.

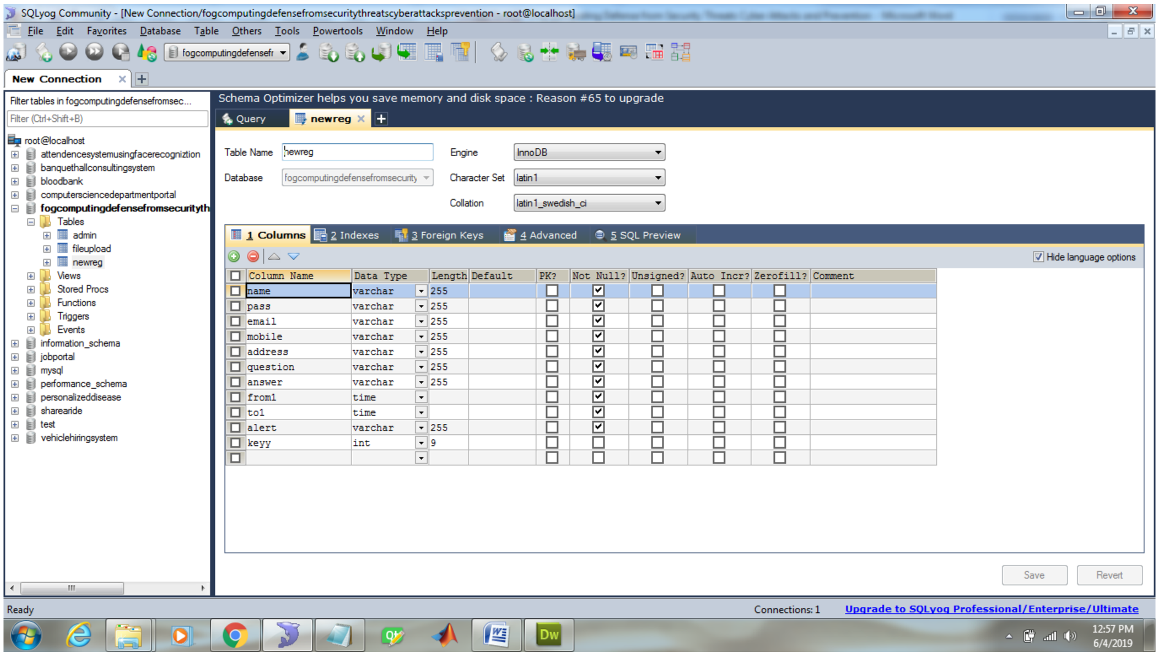
Process Review

It was discovered that this application software package in question is employed in managing all the data desires of the varied hospitals. A program director signs into the program from the underlying interface, makes clients and dole out jobs and availability catches are allocate to the made client. The client presently, signs into the program through the sign in interface with the accreditations from the executive, signs into the program, if approval is fruitful , the client is presently invited into the fundamental program. Figure 3.1 depicts the data framework structure in which the overseer makes clients in each office and appoints client jobs and accreditations dependent on expected set of responsibilities

A purposive inspecting procedure was embraced to particularly set up those that influence the information framework on to elicit their encounters as a guide.

Partner inspecting system which is helpful in recognizing real partners engaged with structuring, giving, getting or executing a program or administration being assessed. This partner was chosen for an organized profundity meet.

Tables



SQLyog Community - [New Connection/fogcomputingdefensefromsecuritythreatscyberattacksprevention - root@localhost]

Schema Optimizer helps you save memory and disk space : Reason #65 to upgrade

root@localhost
- attendencesystemusingfacerecogniztion
- banquethallconsultingsystem
- bloodbank
- computersciencedepartmentportal
- fogcomputingdefensefromsecurityth
  - Tables
    - admin
    - fileupload
    - newreg
  - Views
  - Stored Procs
  - Functions
  - Triggers
  - Events
- information_schema
- jobportal
- mysql
- performance_schema
- personalizeddisease
- shareaide
- test
- vehiclehiringsystem

Table Name: newreg
Database: fogcomputingdefensefromsecurity
Engine: InnoDB
Character Set: latin1
Collation: latin1_swedish_ci

Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	Comment
name	varchar	255		☐	☑	☐	☐	☐	
pass	varchar	255		☐	☑	☐	☐	☐	
email	varchar	255		☐	☑	☐	☐	☐	
mobile	varchar	255		☐	☑	☐	☐	☐	
address	varchar	255		☐	☑	☐	☐	☐	
question	varchar	255		☐	☑	☐	☐	☐	
answer	varchar	255		☐	☑	☐	☐	☐	
from1	time			☐	☑	☐	☐	☐	
to1	time			☐	☑	☐	☐	☐	
alert	varchar	255		☐	☑	☐	☐	☐	
keyy	int	9		☐	☐	☐	☐	☐	
				☐	☐	☐	☐	☐	

Ready — Connections: 1 — Upgrade to SQLyog Professional/Enterprise/Ultimate

File Edit Favorites Database Table Others Tools Powertools Window Help
New Connection
Query
1 Columns 2 Indexes 3 Foreign Keys 4 Advanced 5 SQL Preview
☑ Hide language options
Save
Revert
12:57 PM
6/4/2019

Table 4.1: New User Register Table

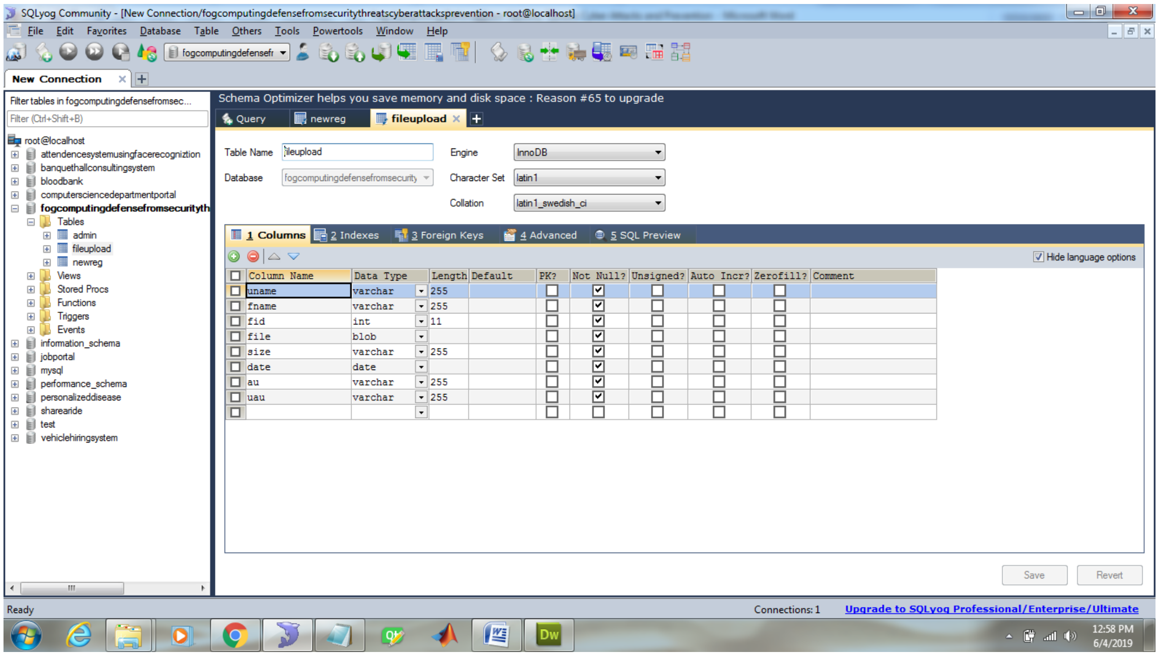
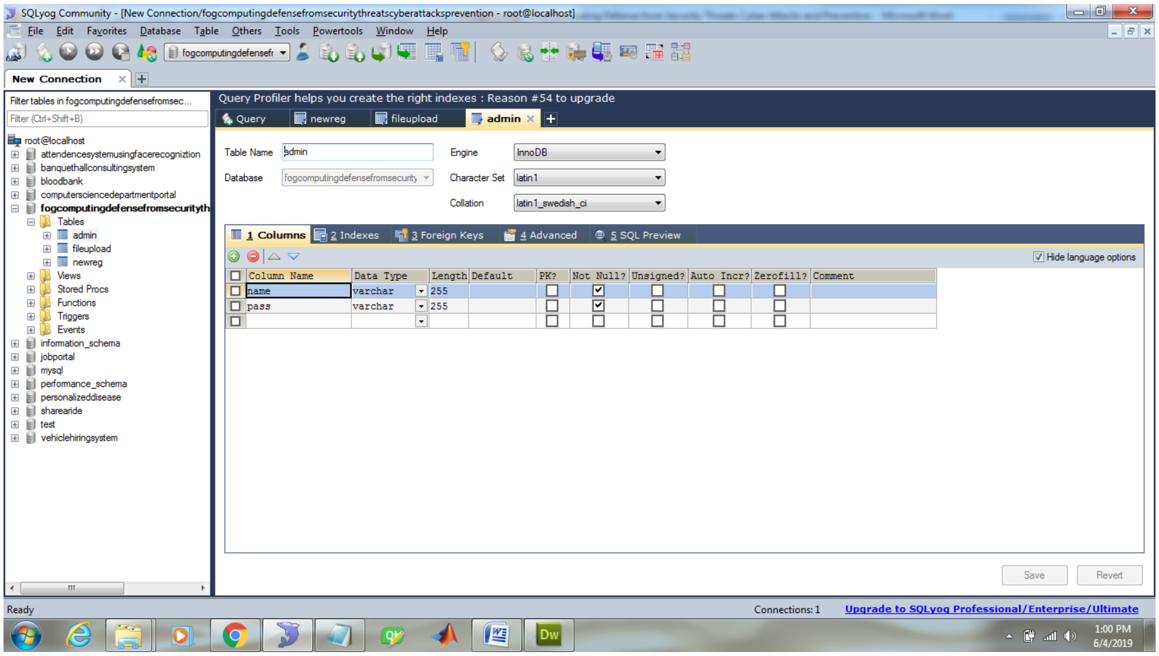

SQLyog Community - [New Connection/fogcomputingdefensefromsecuritythreatscyberattacksprevention - root@localhost]
File Edit Favorites Database Table Others Tools Powertools Window Help
New Connection
Filter tables in fogcomputingdefensefromsec...
Filter (Ctrl+Shift+B)
root@localhost
attendencesystemusingfacerecogniztion
banquethallconsultingsystem
bloodbank
computersciencedepartmentportal
fogcomputingdefensefromsecurityth
Tables
admin
fileupload
newreg
Views
Stored Procs
Functions
Triggers
Events
information_schema
jobportal
mysql
performance_schema
personalizeddisease
sharearide
test
vehiclehiringsystem
Schema Optimizer helps you save memory and disk space : Reason #65 to upgrade
Query
newreg
fileupload
1 Columns
2 Indexes
3 Foreign Keys
4 Advanced
5 SQL Preview
Hide language options
Save
Revert
Ready
Connections: 1
Upgrade to SQLyog Professional/Enterprise/Ultimate
12:58 PM
6/4/2019

Table Name: ileupload
Database: fogcomputingdefensefromsecurity
Engine: InnoDB
Character Set: latin1
Collation: latin1_swedish_ci

□	Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	Comment
□	uname	varchar	255		□	☑	□	□	□	
□	fname	varchar	255		□	☑	□	□	□	
□	fid	int	11		□	☑	□	□	□	
□	file	blob			□	☑	□	□	□	
□	size	varchar	255		□	☑	□	□	□	
□	date	date			□	☑	□	□	□	
□	au	varchar	255		□	☑	□	□	□	
□	uau	varchar	255		□	☑	□	□	□	
□					□	□	□	□	□	

Table 4.2: User Upload Data to Cloud.



SQLyog Community - [New Connection/fogcomputingdefensefromsecuritythreatscyberattacksprevention - root@localhost]

Query Profiler helps you create the right indexes : Reason #54 to upgrade

Filter tables in fogcomputingdefensefromsec...

root@localhost
- attendencesystemusingfacerecogniztion
- banquethallconsultingsystem
- bloodbank
- computersciencedepartmentportal
- fogcomputingdefensefromsecurityth
  - Tables
    - admin
    - fileupload
    - newreg
  - Views
  - Stored Procs
  - Functions
  - Triggers
  - Events
- information_schema
- jobportal
- mysql
- performance_schema
- personalizeddisease
- shareaide
- test
- vehiclehiringsystem

Table Name: admin
Database: fogcomputingdefensefromsecurity
Engine: InnoDB
Character Set: latin1
Collation: latin1_swedish_ci

☑ Hide language options

□	Column Name	Data Type	Length	Default	PK?	Not Null?	Unsigned?	Auto Incr?	Zerofill?	Comment
□	name	varchar	255		□	☑	□	□	□	
□	pass	varchar	255		□	☑	□	□	□	
□					□	□	□	□	□	

Ready   Connections: 1   Upgrade to SQLyog Professional/Enterprise/Ultimate

1:00 PM
6/4/2019

Table 4.3: User Upload Data to Cloud.

CHAPTER IV
ANALYSIS AND DESIGN

Introduction

After a cautious investigation of the framework, procedures and strategies of the current data framework being used, the accompanying issues which were found were considered to have huge significance to the case under examination. The framework was seen not to have any review trailing procedure and technique considering the nature and condition inside which it works (distributed computing condition). Another region important to this examination was a review and observing trail measure, it was appeared at have any framework set up that reviews and screens framework clients and this implied client exercises couldn't be followed or checked for inspecting and security appraisal purposes using an exchange log screen. Notwithstanding, it supposedly had a legitimately characterized client job definitions and openness works set up which set clients into their jobs dependent on sets of expectations.

The design document that we'll develop throughout this part is that the blueprint of the code .

It describes however the answer to the client drawback is to be designed.

Since answer to advanced issues isn’t sometimes found within the 1st attempt, iterations area unit possibly needed.

Three types of decisions: -

Define the boundaries along which to break; Determine into how money pieces to break; and Identify the right level of detail once style ought to stop and implementation ought to begin. Basic design principles that enable the software engineer to navigate the design process suggest a set of principles for software design, which have been adapted and extended in the following list: Free from the suffer from "tunnel vision." an honest designer ought to take into account various approaches, making every supported necessities of the matter, the resources accessible to try and do the task.

Because one component of look model usually traces to multiple necessities, it is necessary to have a means for tracking how requirements have been satisfied by the design model. The design should not repeat the same thing. Systems area unit created employing a set of style patterns, many of which have likely been encountered before. These patterns must always be chosen as another to reinvention. Time is short and resources are limited! Design time ought to be endowed in representing actually new ideas and integration those patterns that exist already.

The design ought to "minimize the intellectual distance" between the computer code and therefore the downside because it exists within the globe.

The design should exhibit uniformity and integration. A style is uniform if it seems that one person developed the whole issue. Rules of favor and format ought to be outlined for a style team before style work begins. A style is integrated if care is taken in shaping interfaces between style parts

The design activity begins once the wants document for the software package to be developed is offered. This may be the SRS for the entire system, as is that the case if the falls model is being followed or the wants for future "iteration" if the iterative sweetening is being followed or the wants for the model if the prototyping is being followed. While the specification is entirely within the drawback domain, style is that the opening in moving from the matter domain toward the answer domain. Design is actually the bridge between needs specification and also the racial extermination for satisfying the wants.

The design of a system is actually a blueprint or a concept for an answer for the system. We contemplate a system to be a collection of elements with clearly outlined behavior interacts and very mounted outlined manner to provide some behavior or services for its environment. A part of a system is thought of a system, with its own elements. In a software, a part could be a software system module.

The design method for software systems has 2 levels. At the primary level, the main focus is on deciding that modules area unit required for the system, the specifications of those modules, & the way modules ought to be interconnected. In the second level, the interior style of the modules, or however the specifications of the module are glad, is decided. This style level is usually referred to as careful style or logic style. Detailed style primarily expands the system style to contain careful description of the process logic and information structures so the look is sufficiently complete for writing.

.The system style incorporates a major impact on the testability and modifiability of a system, and it impacts its potency. Much of (the style/the planning/the look) effort for coming up with software package is spent making the system design.

The input to the look section is that the specifications for the system to be designed .Hence, reasonable entry criteria can be that the specifications are stable and have been approved, hoping that the approval mechanism will ensure that the specifications are complete, consistent, unambiguous, etc. The output of the top-ranking style section is that the field of study style or the system style for the software package to be engineered,and can be created with or while not employing a style methodology. Reasonable exit criteria for the phase could be that the design has been verified against the input specifications and has been evaluated and approved for quality.

A design can be object-oriented or function-oriented. In function-oriented style, the planning consists of module definitions, with every module supporting a purposeful abstraction. In object-oriented style, the modules within the style represent information abstraction (these abstractions area unit mentioned in additional detail later). In the function-oriented strategies for style and describe one explicit methodology the structured style methodology in some detail. In a function- adjusted style approach, a system is viewed as a metamorphosis perform, transforming the inputs to the desired outputs. The purpose of the planning section is to specify the parts for this transformation perform, in order that every parties additionally a metamorphosis perform. Hence, the essential output of the system style section, once a perform adjusted style approach is being followed, is the definition of all the major data structures in the system, all the key modules of the system, and the way the modules act with one another. Once the style/|the planning the looker is happy with the design he has made, the planning is to be exactly laid out in the shape of a document. To specify the design, specification languages are used. Producing the planning specification is that the final objective of the planning section. The purpose of this style document is sort of completely different from that of the planning notation.

PROPOSED SYSTEM

We propose a different approach for securing data in the server using offensive decoy technology. We monitor data access in the Fog and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack to the attacker. This protects against the misuse of user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user data security in a server environment. We propose a completely different approach to securing the server using decoy information technology, that we have come to call Fog Computing. We use this technology to launch disinformation attacks against
malicious insiders, preventing them from distinguishing the real sensitive
user's data from fake worthless data.

4.1.2 System Design

Following those discoveries produced using the current application programming, another plan which looks to address the deficits found was made to incorporate exchange log exercises pointed a checking client exercises inside a framework with an end goal to address character and openness dangers.

Database

To guarantee the security of the new framework, a progressively organized MYSQL database framework with a solid database secret phrase coded in the program source code was utilized. A social database the executives framework (RDBMS) created by Apache Programming Establishment which can be implanted in java programs and utilized for online exchange preparing was utilized in this advancement. Derby's database motor backings Java database network (JDBC) and Organized Question Language (SQL) as application programming interfaces. It utilizes IBM DB2 SQL language structure. Derby's system server builds the scope of the database motor by giving conventional Operators server usefulness. It permits Specialist associations over exchange control convention over web convention (TCP/IP) utilizing standard Dispersed Social Database Engineering convention. The system server enables Derby motor to help Arranged JDBC, ODBC-CLI, PERL and JSP.

This installed system server has some significant points of interest which are; it very well may be arranged to go about as a mixture server/inserted RDBMS to acknowledge TCP/IP associations from different Operators indicated notwithstanding Specialists inside a similar java virtual machine (JVM). It enables one to indicate the accurate database area inside the programming condition of “jdbc : derby://localhost:8082/"c:\private\tmp\databasename; user="root"; password=pass secret key. This implies no different database application; all databases including database

Tables, conditions and so forth are inserted inside the coding framework structure. This database approach has a great deal of favorable circumstances despite the fact that it exhibits some dimension of test as it takes into account an alternate database area to be indicated other than the advancement condition

System Model

Numerous models were assessed to all the more likely comprehend the framework and what it should do and furthermore to exhibit the sort of relations that should exist between the different segments of the undertaking. Among the models assessed in this undertaking are the element social graphs, information stream chart, setting outline, prerequisite use case graph and a key based graph however the one which most fits into this advancement model was the element social.

Element Social Outlines: In the element social connections in this task, there is an immediate connection between the Client and program Openness choices. The client's validation decides his/her availability into the product code. Whenever validated, it demonstrates that the client has been properly checked dependent on certifications contained in the archive database framework

Crowfoot entity relational diagram

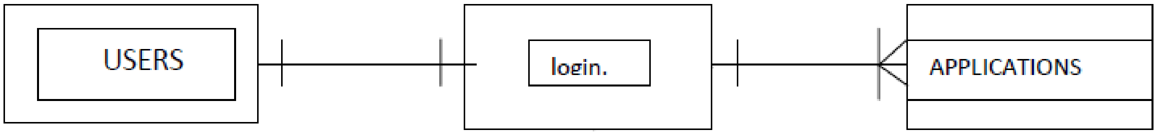


Figure 2.5 Crowfoot entity relational diagram

Figure 2.5 demonstrates the substances and the connections that exist between them. A one-one relationship among clients (1:1), a one numerous connections (1: M) which exist between client Sand either an application or numerous applications. A client can be confirmed once to get to one application or numerous applications with his/her qualifications.

TOOLS / PLATFORM, HARDWARE AND SOFTWARE REQUIREMENT SPECIFICATION

HARDWARE

Processor	**:**	Pentium 2.4 GHz or above
Memory	**:**	256 MB RAM or above
Cache Memory	**:**	128 KB or above
Hard Disk	**:**	3 GB or above [at least 3 MB free space Required]
Pen Drive	**:**	5 GB
Printer	**:**	Laser Printer

SOFTWARE

Operating System	**:**	Windows XP (Professional)./windows 7/8/10
Font-End Tool	**:**	Java/JSP ,Java Script, HTML
Back-End	**:**	MYSQL
Server	**:**	Tomcat 7

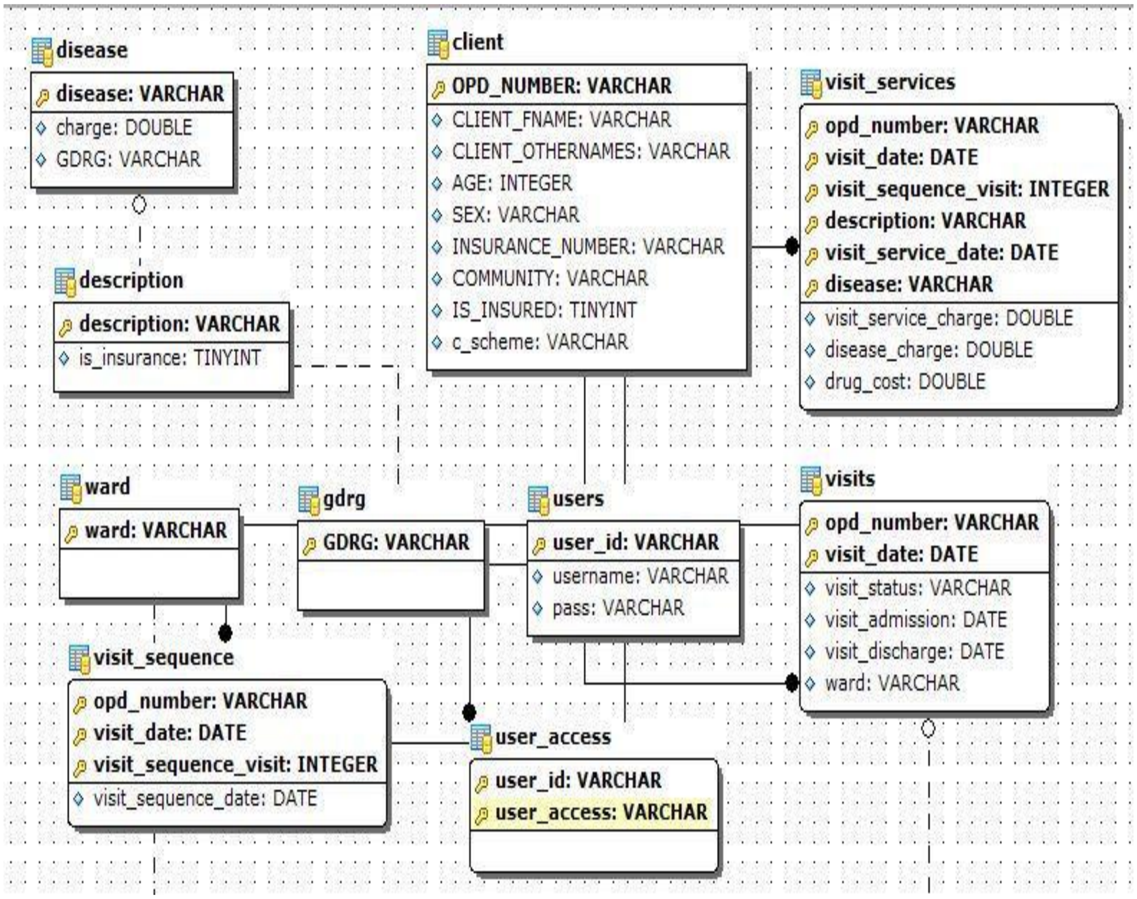


Figure 2.6: Entity Relationship of the database structure

Attributed Entity-Relational Diagram

The E-R outline in Figure 4.3 , shows the substances and the different traits they contain and the relationship that exists between them. It likewise demonstrates all fields and the key fields including both the essential keys and the outside keys related with the different substances. To guarantee that this venture is additionally created to incorporate application programming, a portion of the database fields have been named to take into account simple mix amid coding.

Database Normalization

Standardization is the Quick procedure of proficiently arranging information in a database. The main Typical (1NF), takes out copy segments from a similar table and makes separate tables for each gathering of related information and furthermore recognize each line with a novel section (the essential key). The Second Typical Structure (2NF), endeavors to lessen the measure of excess information in a table y removing it, setting it in new table(s) and making connection between those tables using remote keys. The Third Ordinary Structure (3NF), meet the necessities of both 1NF and 2NF and furthermore to expel segments that are not completely subordinate upon the essential key. All tables/relations inside the database were standardized up to third typical structure since the goal of standardization was acknowledged at the third ordinary structure.

Documentation of the System

The improvement of this framework does not at all influence the structure of the data framework being utilized by these Clinics. It just tries to exhibit the capacity of utilization programming to catching client exercises which can be connected to client openness of figuring assets. It has made a security dimension of the product application to screen and track and review client exercises. It starts with a regulatory formation of a client with the vital accreditations (individual record, client id, secret word and so forth.) and the doling out of the client's availabilities. A client with approval starts at the login interface and enters his/her client name and secret word, after which he/she is taken to the primary program interface to start work. Confirmed, the client is offered access to any product program with available accreditations. Be that as it may, if the approval is fruitless, a client is provoked with a message exchange showing an approval disappointment.

CHAPTER V

Conclusion

Fog security is one of the major important point to be considered in Fog computing. Masquerade or insider is the person who behaves as a normal user by stealing credentials of authorized person. Insider attack is very difficult to diagnose. So the given approaches help to provide the higher and intelligent level of security in terms of insider attacks. The approaches are based on the predefined user behaviors and monitoring as well as profiling it using decoys. In case of abnormal behavior i.e. insider attack, decoy documents are presented to the user which is actually a bogus information. These decoy documents can also be checked to detect such insider attack. Thus using these approaches the very important and hard to detect attack i.e. insider attack can be handled and the data can be very well secured. The false positive percentage for these approaches is very low.

We present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone’s documents in a Cloud service. Decoy documents stored in the Cloud alongside the user’s real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user’s real data. Such preventive attacks that rely on disinformation technology ,could provide unprecedented levels of security in the Cloud and in social networks

Cost and Benefit Analysis

Information escape is brought about by inward and outside gatherings, either by plan or inadvertently.

As per INFOWATCH's "Worldwide information escape Report, 2009" fifty one of learning spillages were come about because of purposeful assaults and forty third of the spillages were a result of inadvertent occasions, that shows a solid increment on deliberate spillages as contrasting with 2007 figures (for example 29% deliberate and 71% coincidental). Per this investigation by INFOWATCH it tends to be concluded that information spillages is costing associations a great deal of cash, through data breaks, so it is increasingly valuable to mount a framework to follow all exercises of clients into a framework.

Recommendation

It is prescribed that establishments ought to have the capacity to verify programs that will enable heads to follow all exercises of clients into their framework. Its exchange log following framework will guarantee non-disavowal of passage and utilization of administration as each exchange (check) is caught and showed in the log. Its utilization by chiefs engaged with wellbeing basic applications inside Cloud situations will guarantee that information spillage is checked, framework interruption is controlled, client availabilities are appropriately overseen and review trail improvements. By this clients will forgo odious exercises since they realize that they are being viewed.

Restrictions of the New Framework

The examination did not harp on confirmation, for instance biometric check, before getting entrance into the framework. The framework did not give the manager the opportunity to track or screen all exercises of clients remotely.

Future Activities

Sooner rather than later a cloud framework will be verified to in order to screen clients remotely and furthermore to know whether clients can spill information whiles behind the machine through Messaging.

Appendices

Chapter one (1) is the beginning which gives a brief contextual set to the lessons .

Chapter Two (2) is the Literature appraises and reviews literature about like works others have done on the subject of the work.

Chapter Three (3) is the Methodology of the research matter.

Chapter Four (4) is the Analysis and aim, whereas

Chapter Five (5) is the conclusion and the summary of the thesis, recommendation and also a proposed future work to be pursue.

REFERENCES

1. *Data Center Companies*, Jul. 2017, [online] Available: https://www.datacenters.com/directory/companies.

2. F. Bonomi, R. Milito, J. Zhu, S. Addepalli, "Fog computing and its role in the Internet of Things", *Proc. 1st Ed. MCC Workshop Mobile Cloud Computer*. *(MCC)*, pp. 13-16, Feb. 2012

3 *Cisco Delivers Vision of Fog Computing to Accelerate Value from Billions of Connected Devices. Press Release*, Jul. 2017, [online] A

4 M. Aazam, E. N. Huh, "Fog computing: The cloud-IOT/IOE middleware paradigm", *IEEE Potentials*, vol. 35, pp. 40-44, May 2016.

[1] Cloud Security Alliance, “Top Threat to Cloud Computing V1.0 ,” March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] M. Arrington, “In our inbox: Hundreds of confidential Twitter documents,” July 2009. [Online]. Available:http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of confidential-twitter-documents.

[3] D. Takahashi, “French hacker who leaked Twitter documents to TechCrunch is busted,” March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked-twitter-documents-to-techcrunch-is-busted/

[4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online]. Available: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwitters-admin-panel/3292

[5] P. Allen, "Obama 's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010. [Online]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html

[6] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.

[7] M. Van Dijk and A. Juels, “On the impossibility of cryptography alone for privacy-preserving cloud computing,” in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec’10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931.1924934

[8] J. Pepitone, “Dropbox’s password nightmare highlights cloud risks,” June 2011.

[9] M. Ben-Salem and S. J. Stolfo, “Modeling user search-behavior for masquerade detection,” in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

[10] B. M. Bowen and S. Hershkop, “Decoy Document Distributor: http://sneakers.cs.columbia.edu/ids/fog/,” 2009. [Online]. Available: http://sneakers.cs.columbia.edu/ids/FOG/

[11] M. Ben-Salem and S. J. Stolfo, “Combining a baiting and a user search profiling techniques for masquerade detection,” in Columbia University Computer Science Department, Technical Report # cucs-018-11, 2011. [Online]. Available:

Sites Referred:

http://java.sun.com

http://www.sourcefordgde.com

http://www.networkcomputing.com/

http://www.roseindia.com/

http://www.java2s.com/

End