



ಕರ್ನಾಟಕ ವಿಜ್ಞಾನ ಮತ್ತು ತಂತ್ರಜ್ಞಾನ ಅಕಾಡೆಮಿ  
ವಿಜ್ಞಾನ ಮತ್ತು ತಂತ್ರಜ್ಞಾನ ಇಲಾಖೆ, ಕರ್ನಾಟಕ ಸರ್ಕಾರ  
**KARNATAKA SCIENCE AND TECHNOLOGY ACADEMY**  
Department of Science and Technology, Government of Karnataka

# CYBER SECURITY: TECHNOLOGIES AND ACADEMIC OPPORTUNITIES

GAJENDRA DESHPANDE

KLS Gogte Institute of Technology, India

**12 June 2020**

<https://gcdeshpande.github.io>

# Contents

---

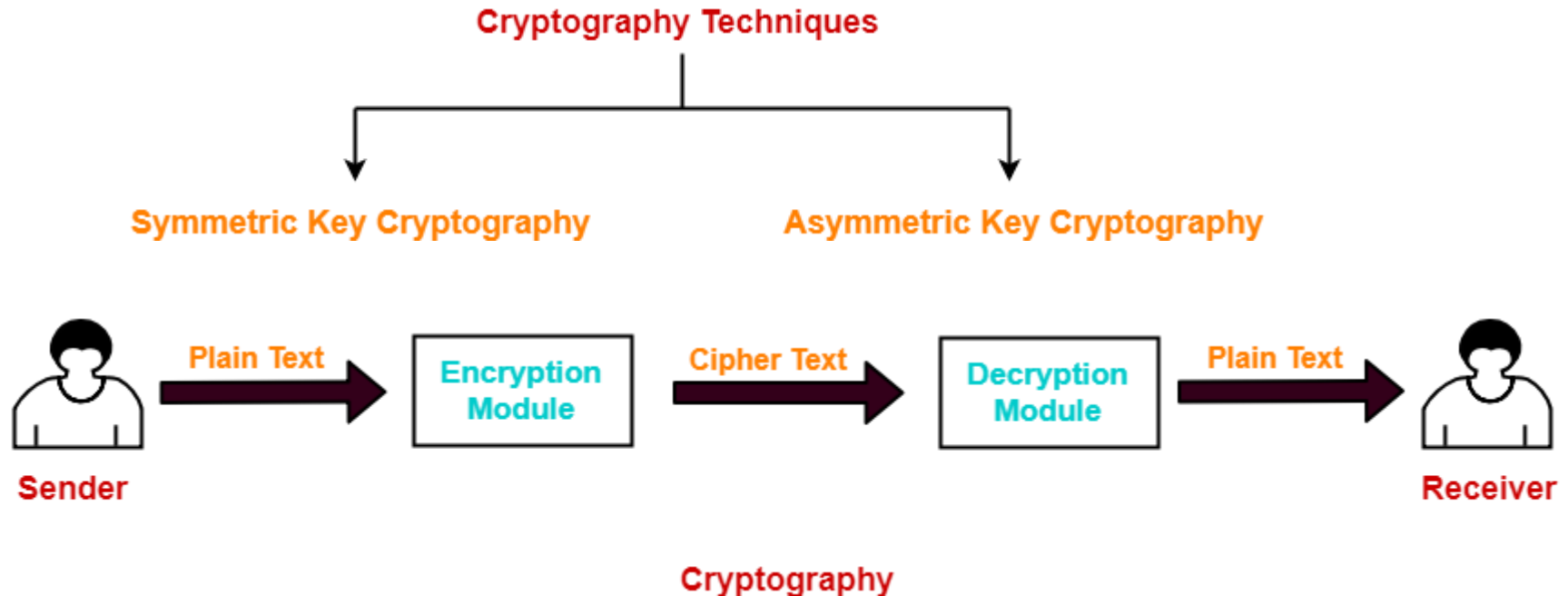
- ▣ Technologies
- ▣ Six security goals
- ▣ Confidentiality
- ▣ Authentication
- ▣ Deception
- ▣ Academic opportunities
- ▣ Starting your own community

# Six Security Goals

- ❑ **Confidentiality:** Only the receiver or user is able to understand the contents of the message.
- ❑ **Authentication:** The identity of the individuals involved can be confirmed.
- ❑ **Accountability and non-repudiation:** Simply an adjunct to authentication.
- ❑ **Integrity:** The assurance that the information has not been altered by elements along the communication path.
- ❑ **Access control:** A security measure that permits access to the various resources by the user or process.
- ❑ **Availability:** The required services must be accessible and available to those users and processes that are permitted to use the information infrastructure.

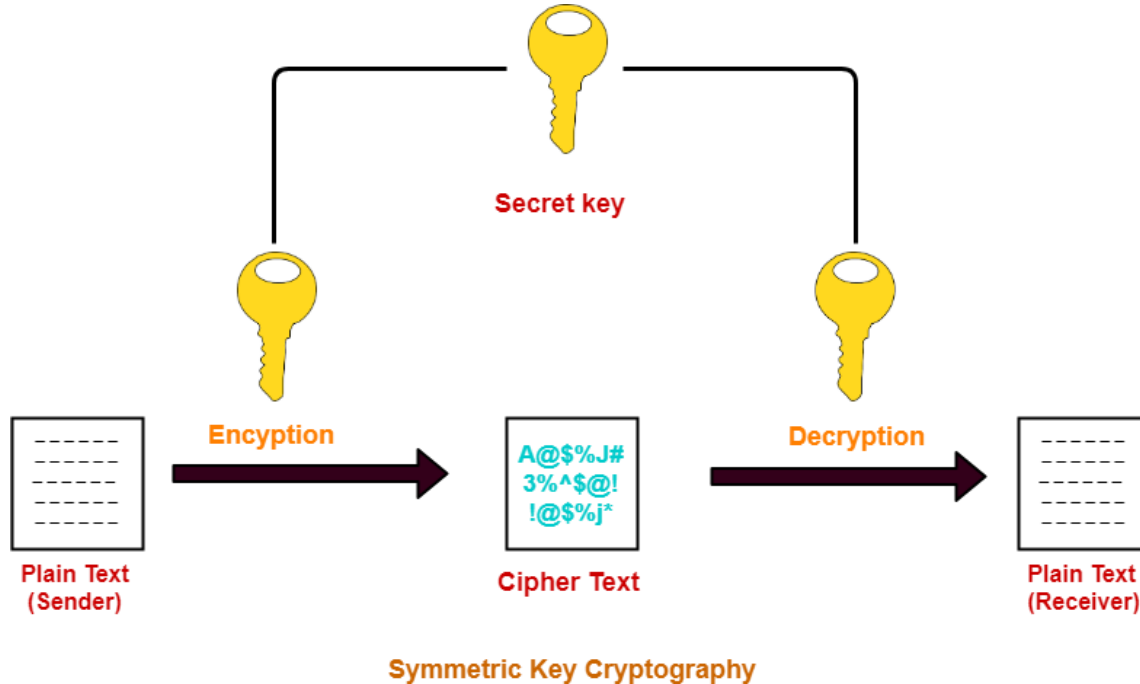
# Confidentiality - Encryption

- Encryption: Converting plain text to cipher text using mathematical formula



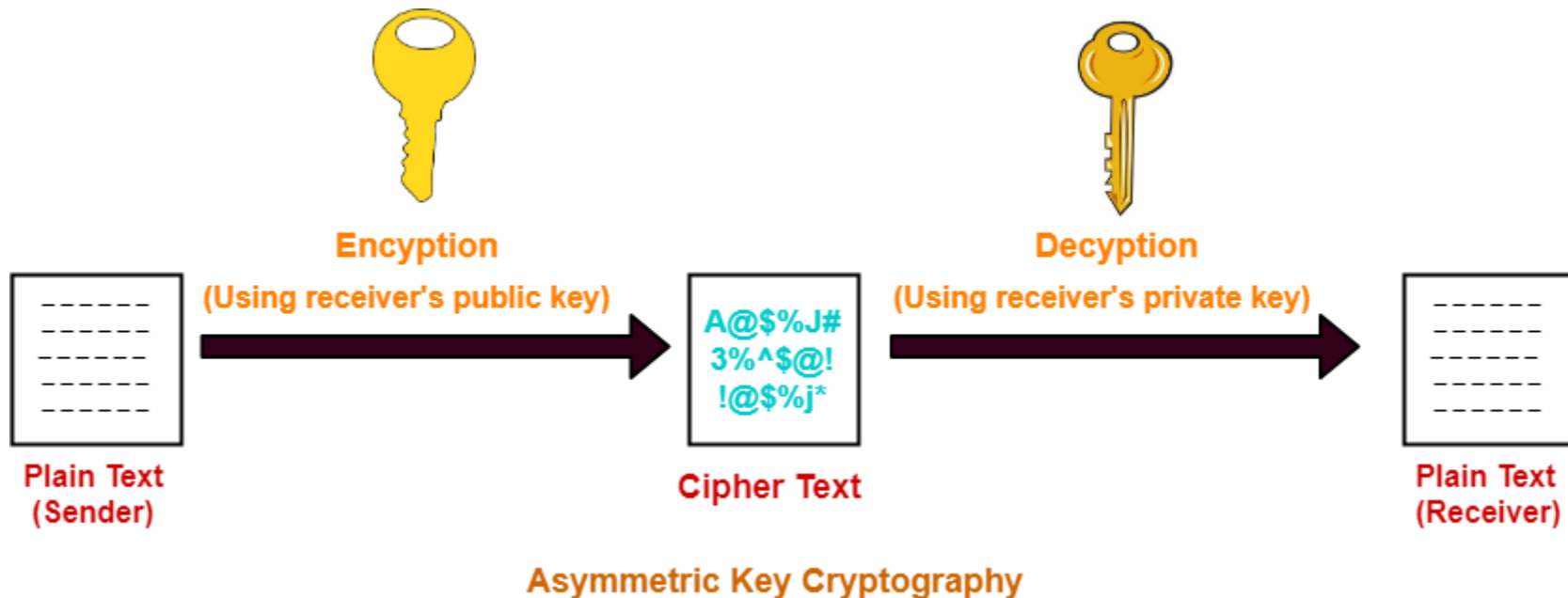
# Confidentiality - Encryption

- Symmetric Key Cryptography: Same key is used for encryption and decryption

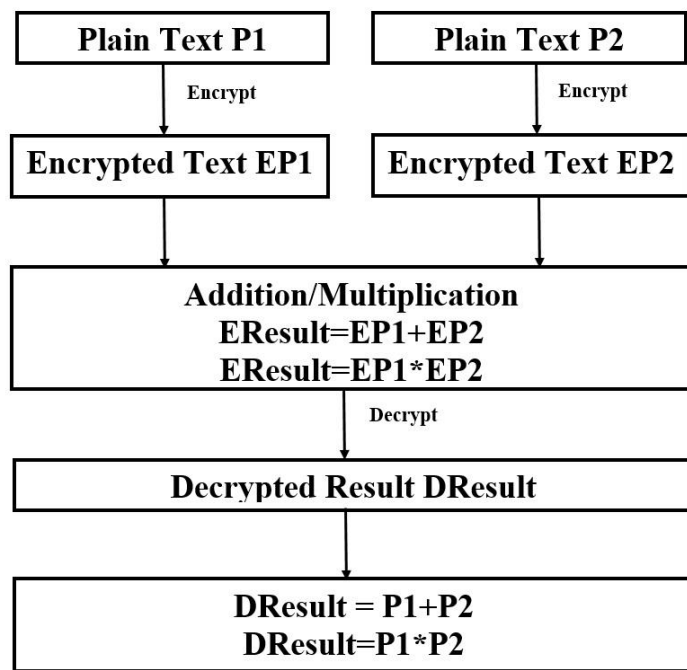


# Confidentiality - Encryption

- Asymmetric Key Cryptography: Different keys are used for encryption and decryption



# Homomorphic Encryption



- $P1=5; P2=10$
- $EP1=50 \ EP2=100$
- $EResult1=50+100=150;$   
 $Eresult2=50*100=5000$
- $DResult1=15;$   
 $DResult2=50$

ActivitiesTerminalNov 2 07:14gajendra@gajendra-HP-Laptop-15-da0xxx: ~/Desktop/scipy 2019/Scipy

```
(base) gajendra@gajendra-HP-Laptop-15-da0xxx:~/Desktop/scipy 2019/Scipy$ python2 rsakar.py
First list of random numbers
[22]

Second list of random numbers
[87]

0.421537876129
0.391266107559
0.39028096199
0.389554977417
0.389764070511
0.389742851257
('N = ', 3125743, '\ne = ', 5)
Encryption of First list of Random numbers
[2027889]

Encryption of Second list of Random Numbers
[1774865]

Decryption of First list of Random Numbers
[22]

Decryption of Second list of Random Numbers
[87]

Product of Two Encrypted Lists
[[3599229209985]]

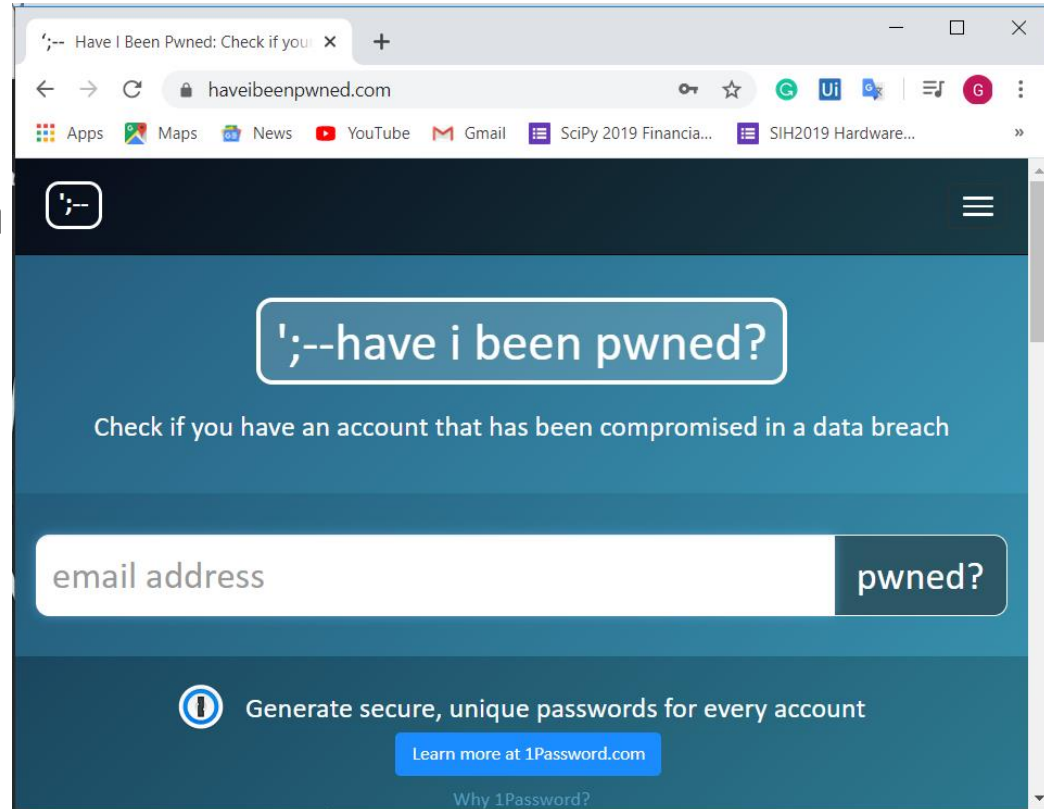
Product of Two Decrypted Lists
[[1914]]

Decryption of Product of Encrypted Lists
[1914L]
```

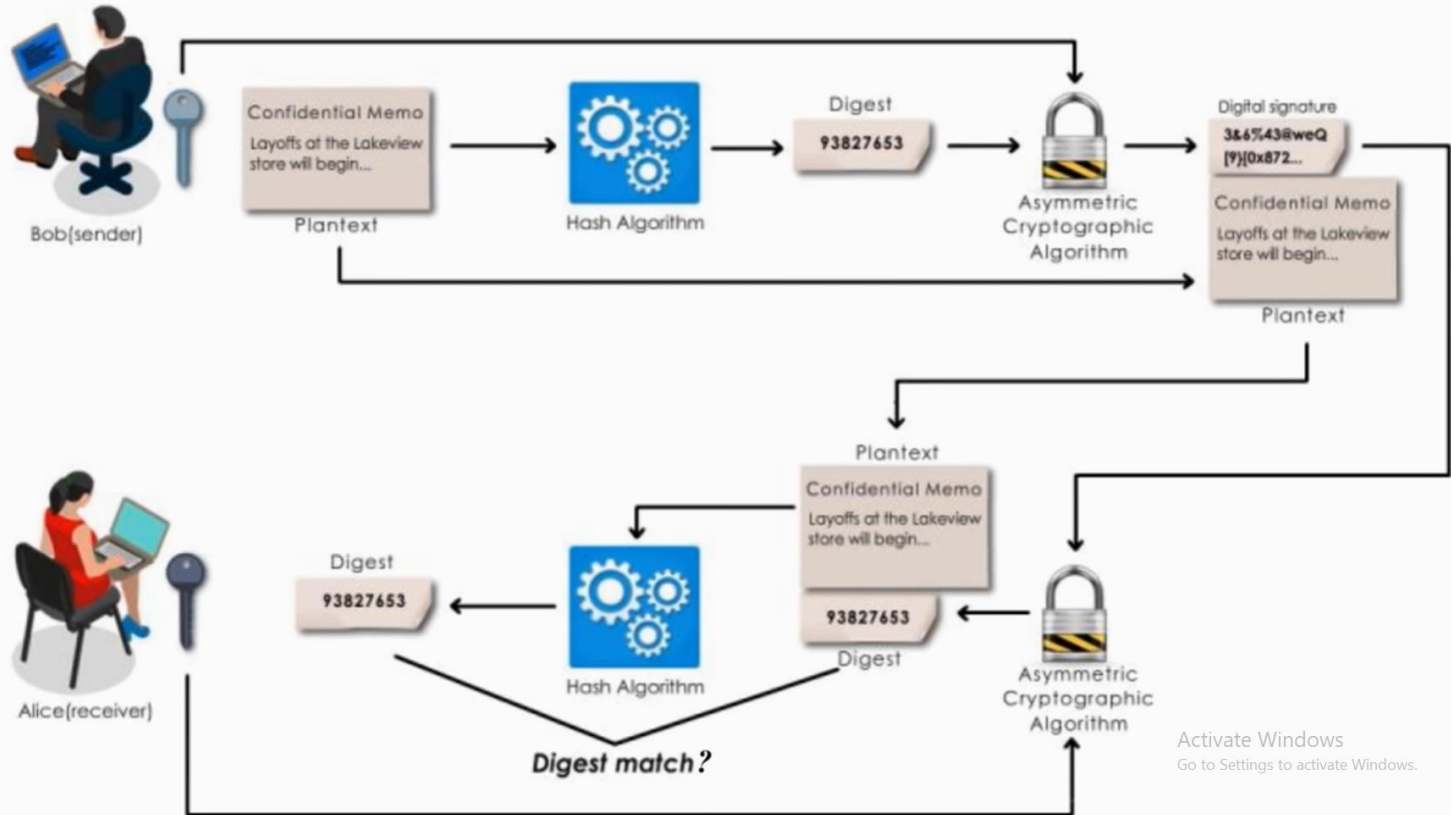


# Authentication

- Passwords
- Two-factor authentication
- Keystroke Dynamics



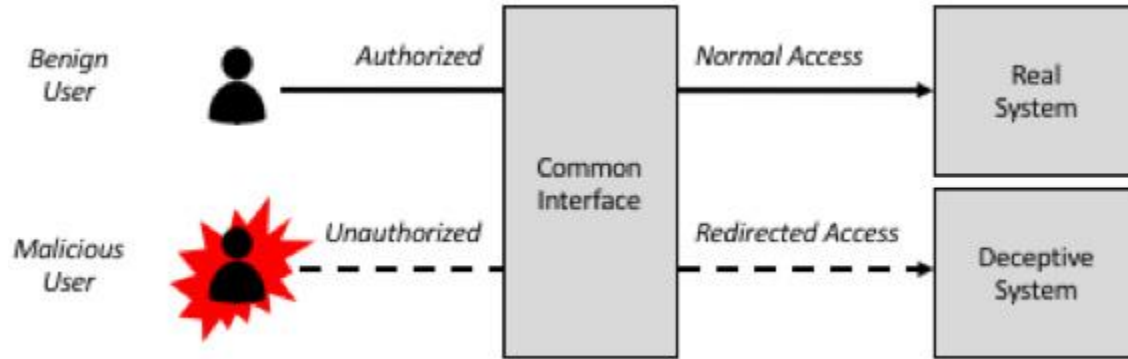
# Integrity – Digital Signature



Activate Windows  
Go to Settings to activate Windows.

# Deception – Basic Idea

- Deception is a technique where hackers methods will be used as security mechanism i.e., phishing the phishers.
- Deception is military tactic used by both attackers and defenders.



Source: <https://www.helpnetsecurity.com/2018/12/06/introduction-deception-technology/>

# Deception – Types

There are two types of Deception Technology described below.

- ❑ **Active Deception:** Active Deception will provide inaccurate information intentionally to the subjects (intruders or hackers) to fall for the trap.
- ❑ **Passive Deception:** Passive Deception will provide incomplete information, other half of information. Intruders will try to gain all the information and then fall for the trap.

Source: <https://www.geeksforgeeks.org/deception-technology/>

They can also be classified as

- ❑ Client side deception – used by hackers
- ❑ Server side deception – used by security providers

**Better Deception = Active Deception + Passive Deception**

# Deception – Evolution - Advantages

- HoneyPots (1998) → HoneyNets(2000) → HoneyToken (2003) → HoneyPot 2.0 (2012) → Deception Technology (2016)
- Advantages
  - Increased accuracy
  - Minimal investment
  - Future ready (applicable to new technology)

# System Design

## Some valid inputs:

Email-id

Mobile number

Alphanumeric word

## Some malicious inputs:

'1 or 1=1

user' or 'a'='a

%00

## Some invalid inputs:

Very large input string

String with special characters

String formed from different character set

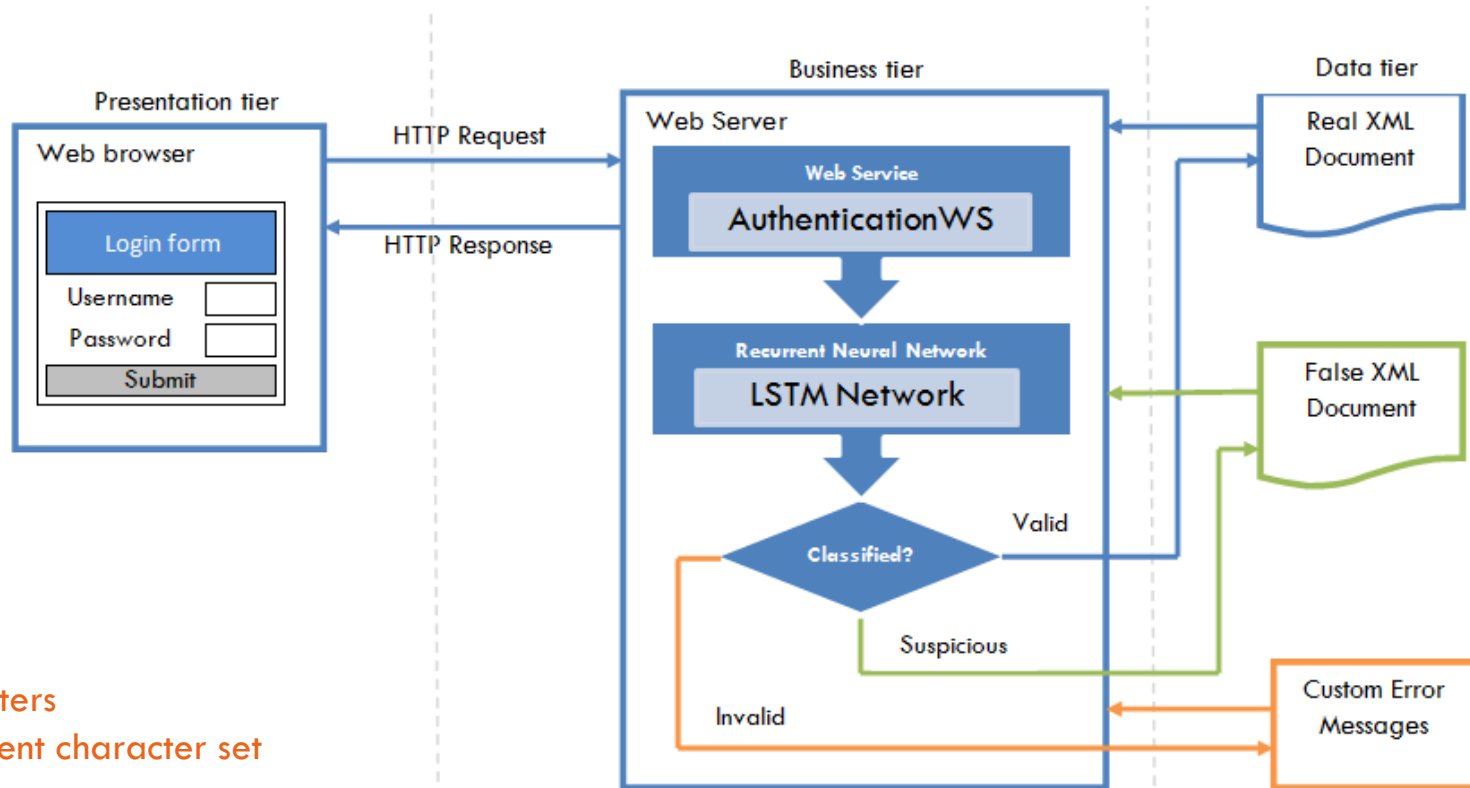
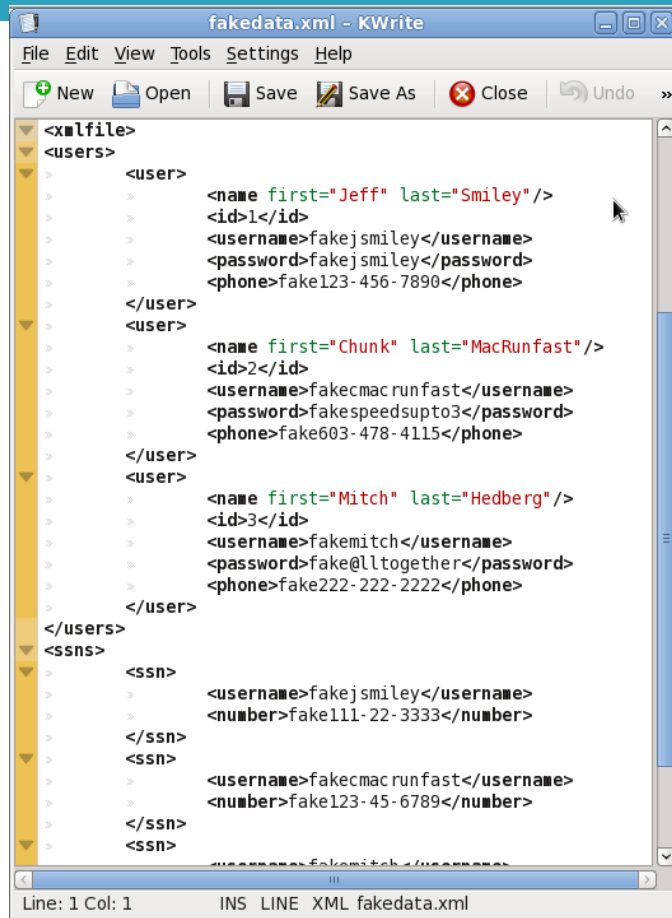


Fig. 1: Three tier architecture of the proposed system

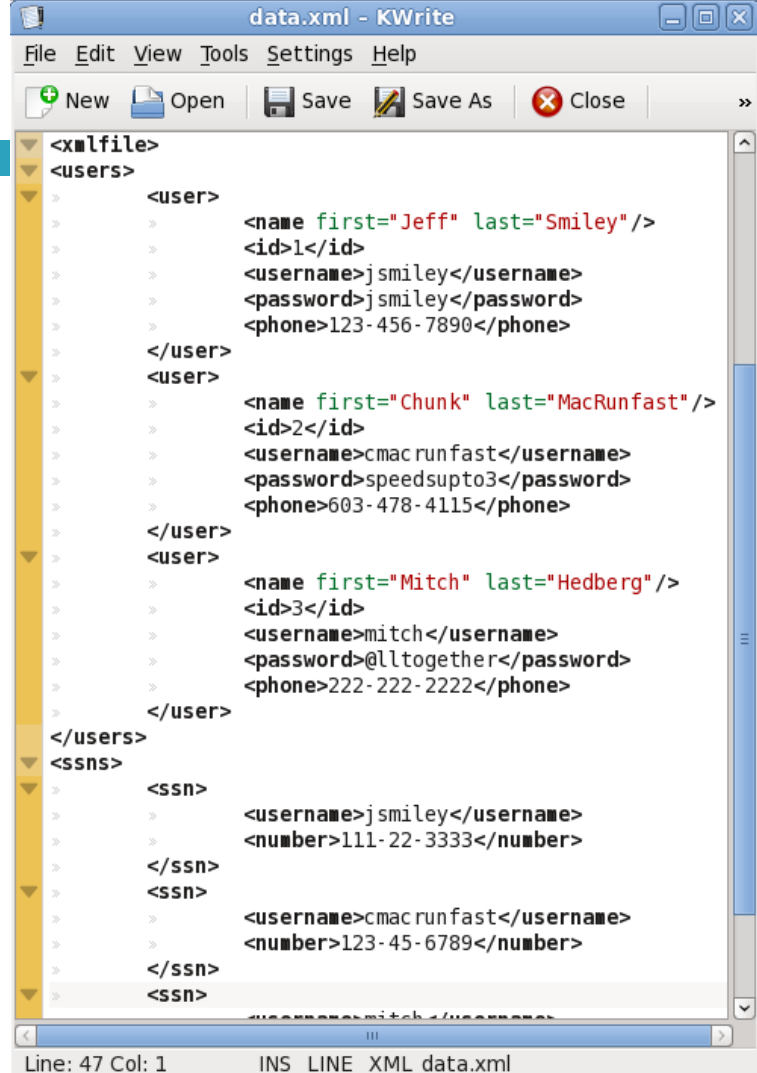
# Snapshots



A screenshot of the KWrite text editor window titled "fakedata.xml - KWrite". The window has a menu bar with "File", "Edit", "View", "Tools", "Settings", and "Help". Below the menu bar is a toolbar with icons for "New", "Open", "Save", "Save As", "Close", and "Undo". The main text area displays XML code for a file named "fakedata.xml". The code is structured with a root element "<xmlfile>" containing two main sections: "<users>" and "<ssns>". The "<users>" section contains three user entries, each with attributes for name, id, username, password, and phone. The "<ssns>" section contains two social security number entries, each with attributes for username and number. The status bar at the bottom indicates "Line: 1 Col: 1" and "INS LINE XML fakedata.xml".

```
<?xml version="1.0"?>
<xmlfile>
  <users>
    <user>
      <name first="Jeff" last="Smiley"/>
      <id>1</id>
      <username>fakejsmiley</username>
      <password>fakejsmiley</password>
      <phone>fake123-456-7890</phone>
    </user>
    <user>
      <name first="Chunk" last="MacRunfast"/>
      <id>2</id>
      <username>fakecmacrunfast</username>
      <password>fakespeedsup3</password>
      <phone>fake603-478-4115</phone>
    </user>
    <user>
      <name first="Mitch" last="Hedberg"/>
      <id>3</id>
      <username>fakekmitch</username>
      <password>fake@lltogether</password>
      <phone>fake222-222-2222</phone>
    </user>
  </users>
  <ssns>
    <ssn>
      <username>fakejsmiley</username>
      <number>fake111-22-3333</number>
    </ssn>
    <ssn>
      <username>fakecmacrunfast</username>
      <number>fake123-45-6789</number>
    </ssn>
    <ssn>
      <username>fakekmitch</username>
      <number>fake222-222-2222</number>
    </ssn>
  </ssns>
</xmlfile>
```

Line: 1 Col: 1    INS LINE XML fakedata.xml



A screenshot of the KWrite text editor window titled "data.xml - KWrite". The window has a menu bar with "File", "Edit", "View", "Tools", "Settings", and "Help". Below the menu bar is a toolbar with icons for "New", "Open", "Save", "Save As", "Close", and "Undo". The main text area displays XML code for a file named "data.xml". The code is structured with a root element "<xmlfile>" containing two main sections: "<users>" and "<ssns>". The "<users>" section contains three user entries, each with attributes for name, id, username, password, and phone. The "<ssns>" section contains two social security number entries, each with attributes for username and number. The status bar at the bottom indicates "Line: 47 Col: 1" and "INS LINE XML data.xml".

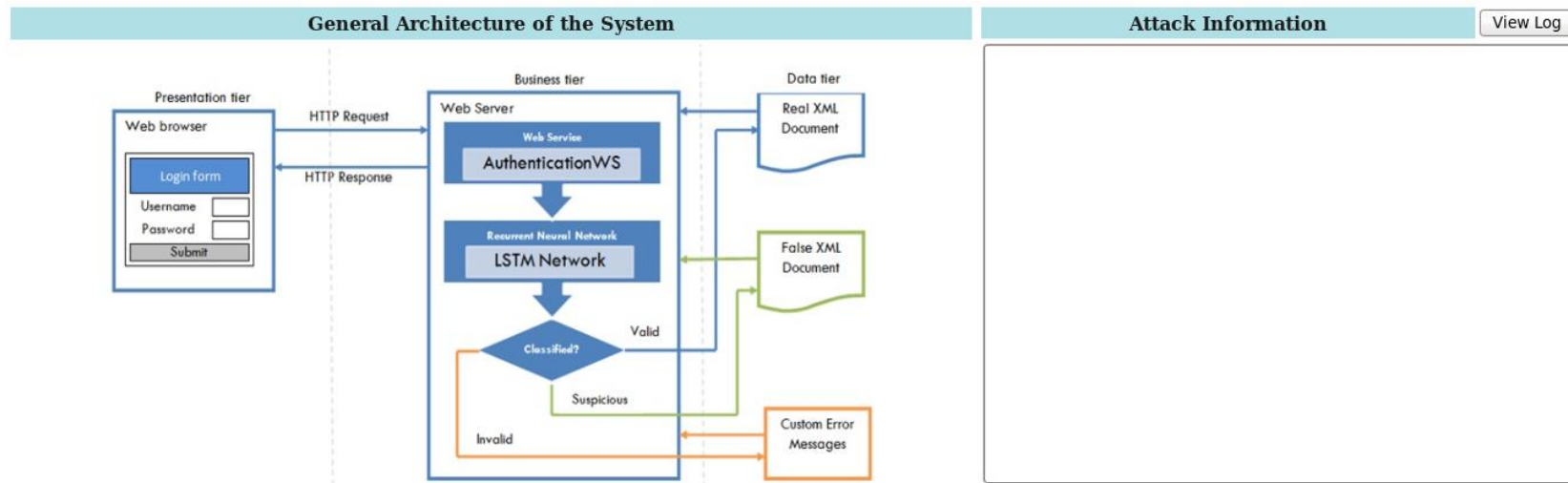
```
<?xml version="1.0"?>
<xmlfile>
  <users>
    <user>
      <name first="Jeff" last="Smiley"/>
      <id>1</id>
      <username>jsmiley</username>
      <password>jsmiley</password>
      <phone>123-456-7890</phone>
    </user>
    <user>
      <name first="Chunk" last="MacRunfast"/>
      <id>2</id>
      <username>cmacrunfast</username>
      <password>speedsup3</password>
      <phone>603-478-4115</phone>
    </user>
    <user>
      <name first="Mitch" last="Hedberg"/>
      <id>3</id>
      <username>mitch</username>
      <password>@lltogether</password>
      <phone>222-222-2222</phone>
    </user>
  </users>
  <ssns>
    <ssn>
      <username>jsmiley</username>
      <number>111-22-3333</number>
    </ssn>
    <ssn>
      <username>cmacrunfast</username>
      <number>123-45-6789</number>
    </ssn>
    <ssn>
      <username>mitch</username>
      <number>222-222-2222</number>
    </ssn>
  </ssns>
</xmlfile>
```

Line: 47 Col: 1    INS LINE XML data.xml

# Snapshots (initial output)

## Implementation of Prevention of XPath Injection Attack using PyBRAIN Machine Learning Library

Login Form	Neural Network Output	Analysis of Results
<p>UserName <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Submit"/> <input type="button" value="Reset"/></p> <div></div>	<div>Click to view the output</div> <div></div>	<div>Analysis of Results</div> <div></div>





# Snapshots (valid input scenario)

## Implementation of Prevention of XPath Injection Attack using PyBRAIN Machine Learning Library

### Login Form

User Name

Password

Submit

Reset

login successful

### Neural Network Output

Click to view the output

epoch	0	total error	0.21833	avg weight	0.99168
epoch	1	total error	0.19241	avg weight	0.99171
epoch	2	total error	0.13013	avg weight	0.99189
epoch	3	total error	0.15396	avg weight	0.99243
epoch	4	total error	0.20026	avg weight	0.99314
epoch	5	total error	0.21473	avg weight	0.99399
epoch	6	total error	0.2222	avg weight	0.99529
epoch	7	total error	0.22216	avg weight	0.99623
epoch	8	total error	0.22222	avg weight	0.998
epoch	9	total error	0.22222	avg weight	1.0001
epoch	10	total error	0.22222	avg weight	1.0029

### Analysis of Results

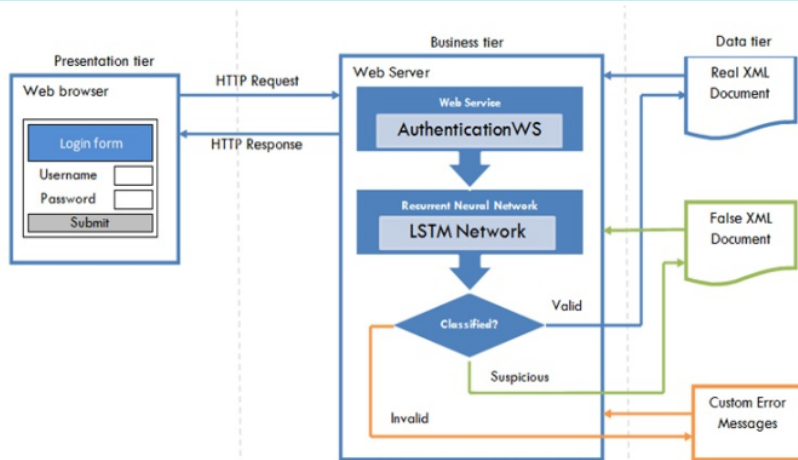
Analysis of Results

Login Attempt: 4

Result of Neural Network 1 (I/P: Error Code; O/P: Class)  
(Number of training patterns: ', 3)  
(Input and output dimensions: ', 2, 3)  
(train error: 0.00%', ', test error: 0.00%')

Result of Neural Network 2 (I/P: Login attempt; O/P: Class)  
(Number of training patterns: ', 4)  
(Input and output dimensions: ', 2, 2)  
(train error: 0.00%', ', test error: 0.00%')

### General Architecture of the System



### Attack Information

[View Log](#)

```
Remote Port: 59968
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user%27%20or%20%27a%27=%27a
Server Time: Tue May 28 16:42:11 2013

Remote Port: 58141
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=&txtPasswd=
Server Time: Tue May 28 16:49:50 2013

Remote Port: 59795
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user
```

# Snapshots (malicious input scenario)

## Implementation of Prevention of XPath Injection Attack using PyBRAIN Machine Learning Library

### Login Form

UserName

Password

### Neural Network Output

Click to view the output

epoch	0	total error	0.21833	avg weight	0.99168
epoch	1	total error	0.19241	avg weight	0.99171
epoch	2	total error	0.13013	avg weight	0.99189
epoch	3	total error	0.15396	avg weight	0.99243
epoch	4	total error	0.20026	avg weight	0.99314
epoch	5	total error	0.21473	avg weight	0.99399
epoch	6	total error	0.2222	avg weight	0.99529
epoch	7	total error	0.22216	avg weight	0.99623
epoch	8	total error	0.22222	avg weight	0.998
epoch	9	total error	0.22222	avg weight	1.0001
epoch	10	total error	0.22222	avg weight	1.0029

### Analysis of Results

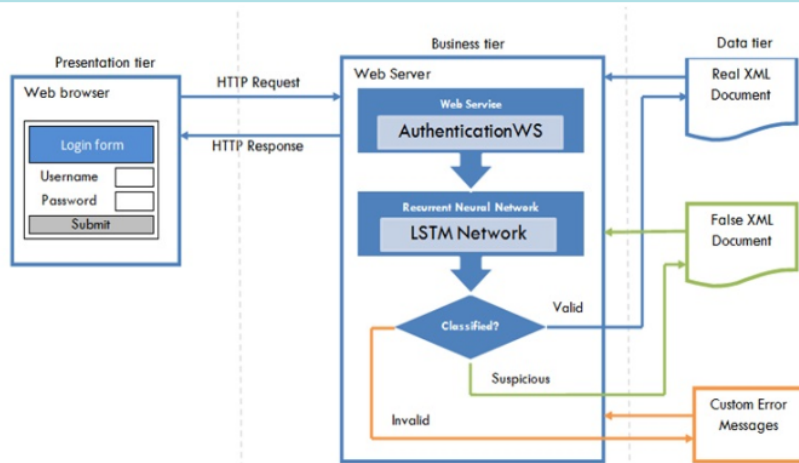
Analysis of Results

Login Attempt: 4

Result of Neural Network 1 (I/P: Error Code; O/P: Class)  
( 'Number of training patterns: ', 3)  
( 'Input and output dimensions: ', 2, 3)  
( 'train error: 0.00%', ', test error: 0.00%')

Result of Neural Network 2 (I/P: Login attempt; O/P: Class)  
( 'Number of training patterns: ', 4)  
( 'Input and output dimensions: ', 2, 2)  
( 'train error: 0.00%', ', test error: 0.00%')

### General Architecture of the System



### Attack Information

View Log

```
Remote Port: 59968
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user%27%20or%20%27a%27=%27a
Server Time: Tue May 28 16:42:11 2013

Remote Port: 58141
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=&txtPasswd=
Server Time: Tue May 28 16:49:50 2013

Remote Port: 59795
Remote Address: 127.0.0.1
Request Method GET
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10)
Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user
```

# Snapshots (fake login scenario)

## Implementation of Prevention of XPath Injection Attack using PyBRAIN Machine Learning Library

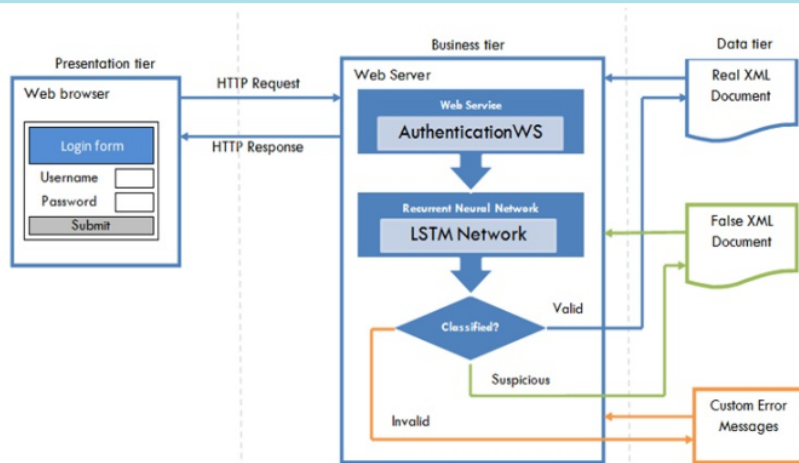
**Login Form**  
UserName   
Password   
   
fake login successful

**Neural Network Output**  

epoch	0	total error	0.21833	avg weight	0.99168
epoch	1	total error	0.19241	avg weight	0.99171
epoch	2	total error	0.13013	avg weight	0.99189
epoch	3	total error	0.15396	avg weight	0.99243
epoch	4	total error	0.20026	avg weight	0.99314
epoch	5	total error	0.21473	avg weight	0.99399
epoch	6	total error	0.2222	avg weight	0.99529
epoch	7	total error	0.22216	avg weight	0.99623
epoch	8	total error	0.22222	avg weight	0.998
epoch	9	total error	0.22222	avg weight	1.0001
epoch	10	total error	0.22222	avg weight	1.0029

**Analysis of Results**  
Login Attempt: 4  
Result of Neural Network 1 (I/P: Error Code; O/P: Class)  
( 'Number of training patterns: ', 3 )  
( 'Input and output dimensions: ', 2, 3 )  
( 'train error: 0.00%', ' ', test error: 0.00%' )  
Result of Neural Network 2 (I/P: Login attempt; O/P: Class)  
( 'Number of training patterns: ', 4 )  
( 'Input and output dimensions: ', 2, 2 )  
( 'train error: 0.00%', ' ', test error: 0.00%' )

### General Architecture of the System



### Attack Information

Remote Port: 59968  
Remote Address: 127.0.0.1  
Request Method GET  
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10) Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10  
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user%27%20or%20%27a%27=%27a  
Server Time: Tue May 28 16:42:11 2013

Remote Port: 58141  
Remote Address: 127.0.0.1  
Request Method GET  
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10) Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10  
Query String: txtName=&txtPasswd=  
Server Time: Tue May 28 16:49:50 2013

Remote Port: 59795  
Remote Address: 127.0.0.1  
Request Method GET  
Web Browser: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.10) Gecko/20101005 Fedora/3.6.10-1.fc14 Firefox/3.6.10  
Query String: txtName=user%27%20or%20%27a%27=%27a&txtPasswd=user

# Academic Opportunities

- ▣ Course Name: M.Tech. Information Security (CSE-IS)
- ▣ College/University: NITK, Surathkal
- ▣ Mode: Full Time, Regular
- ▣ Course Duration: 2 years
- ▣ Course Structure: Theory Courses + Lab + Project Work
- ▣ For more information: <https://cse.nitk.ac.in/programmes>

# Academic Opportunities

- Course Name: Post Graduate Diploma in Cyber Law and Cyber Forensics(PGDCLCF)
- College/University: National Law School of India University (NLSIU), Bangalore
- Mode: Distance Learning
- Course Duration: 1 year
- Course Structure: 4 Theory Courses + Dissertation
- For more information: <http://ded.nls.ac.in>

# Academic Opportunities

- Course Name: Master of Cyber Law and Information Security (MCLIS)
- College/University: National Law Institute University (NLIU), Bhopal
- Mode: Full Time, Regular
- Course Duration: 2 years
- Course Structure: Theory Courses + Dissertation + Internship
- For more information: <https://www.nliu.ac.in/academics-courses/master-of-cyber-law-information-security/>

# Academic Opportunities

- ▣ Course Name: Ph.D. (Cyber Law and Information Security)
- ▣ College/University: National Law Institute University (NLIU), Bhopal
- ▣ Mode: Full Time and Part Time
- ▣ Course Duration : 2 years (as per website)
- ▣ Admission Procedure: Written Test + Interview
- ▣ For more information: <https://www.nliu.ac.in/academics-courses/ph-d/>

# Academic Opportunities

- Course Name: Post Graduate Diploma in Cyber Law (PGDCL)
- College/University: NALSAR University of Law, Hyderabad
- Mode: Distance Learning
- Course Duration: 1 year
- Course Structure: 4 Theory Courses
- For more information: <http://nalsarpro.org/Courses/ONE-YEAR-Post-Graduate-Diploma/Cyber-Laws/About-the-Course>



# Academic Opportunities

- Course Name: M.Tech. in Cyber Forensics and Information Security (SFC)
- College/University: Few Colleges under VTU, Belagavi
- Mode: Full Time
- Course Duration: 2 years
- Course Structure: Course Work + Lab + Seminar+ Internship + Project Work
- For more information: <https://vtu.ac.in/wp-content/uploads/2020/03/sfc.pdf>

# Academic Opportunities

- Some Institutes offer Honors program, and Minors program in Cyber Security
- You are a student (UG/PG), but no formal course at your institute on Cyber Security : Find Professors who are working on Cyber Security
- If you are professional : Join meetup groups/professional chapters in your city.
- Collaborate with people who have similar interests

# Starting your own community

- The Open Web Application Security Project (OWASP) – <https://owasp.org/>
  - International Body (177 Groups world wide)
  - Chapters + Projects
- Null Chapters - <https://null.co.in/>
  - Largest Open Security Community in India (14 chapters)



Thank You

# Widescreen Test Pattern (16:9)

## Aspect Ratio Test

(Should appear  
circular)

4x3

16x9

