RESEARCH ARTICLE OPEN ACCESS

A Robust secure application against server attacks and data tampering to minimize the risk

Mehul Sah [1], Vanshika Singh [2], J. Rene Beulah [3]

Department of Computer Science and Engineering, College of Engineering and Technology,
SRM Institute of Science and Technology,
Kattankulathur, Kanchipuram,Chennai - India.

ABSTRACT

In recent attacks on the banking system are performed to steal the user information, stealing money from the bank, making the banking server compromised, and use users account and sensitive information without authorization. Despite all the measures taken by the banks, there has still been a rise in the number of crimes committed in this sector. To address security concerns and gain user trust and confidentiality, we propose a secure proposed system invoking secure user authentication, automatic intrusion detection, and prevention, securing user sensitive information, secure data transmission to the bank server. For user authentication, we propose e-mail OTP-based user validation. Also, to eliminate unauthorized access brute force attacks is been addressed. The top web vulnerability attack named SQL injection is addressed by proposing automatic intrusion detection, prevention measures. To eliminate bot-based attacks to the bank server in overloading the requests, we use a captcha-based prevention measure. To address the traditional approach-based user-sensitive information storage weakness, we propose a negative password generation technique which is a unique approach in storing user-sensitive information like password, customer relationship number, etc. in the bank server. Once user authentication is made secure, secure data transmission to the bank servers has also been addressed. For each file private random key is been generated and assigned. The key is protected from intruders using RC5 based stream encryption algorithm and data owner files are protected using DES encryption algorithm. The encrypted files are stored in the public cloud storage in a ciphertext format.

Keywords:- For experimental results, a banking-based web application is developed using Java frameworks to integrate the proposed modules.

I. INTRODUCTION

Information Security:

Information security, generally abbreviated to InfoSec, is the process in which data is protected from unwanted access, modification, usage, destruction, or inspection etc. It is a term which is generally used to describe both type of data i.e., physical as well as electronic data.

IT security

It is also known as computer security; it refers to a type of information security which is used to secure technologies (usually some type of information system like computer). It's worthy to notice that a computing device doesn't essentially mean a home desktop. Any device which possesses a processing unit and a bit of memory can be termed as a computer. Computing devices can therefore vary from standalone devices to basic devices like a calculator, to portable devices such as laptops, mobile phones and tablets. IT security requires specialists in most of the major business enterprises/establishments because of the extensive use and storage of valuable data within these big enterprises. They have the responsibility of keeping all of the technology used or developed by the company safe from harmful attacks from the hacker that always try to breach into vital personal and personal info or to gain access to the company's systems or networks.

Information assurance

Information assurance is the process of making sure that information is intact when a critical situation or problem arises. These issues include and are not restricted to instances such as natural calamities, computer/server error, theft etc. where information has the risk of being lost. As most information is kept on computers in today's digital age, information assurance is mostly handled by specialists in the IT security field. Few of the common methods of providing info assurance is to keep backup of the data outside the system to be secure if any of the aforementioned problem occurs.

Threats

Computer system threats are present in many various different forms. A number of the most common threats nowadays are software attacks. It incorporates burglary of licensed innovation, theft of identity, theft of information, sabotage, and coercion of data. Most of individuals these days have encountered a type of a software attack. A couple of the most well-known instances of software attacks are viruses, phishing attacks, Trojan horses, and worms. Furthermore, the robbery of licensed innovation has been a major issue for a few organizations inside the IT field. Intellectual property is the ownership of property for the

most part comprising of some sort of insurance. It is very common to have theft of software in IT business nowadays. Identity theft is the endeavor to demonstration of being some other individual for the most part to get that individual's information or to require benefit of their admittance to significant data. Theft of equipment or info is very common nowadays due to people carrying their mobile phone as the primary device, which is easy to misplace or steal. Cell phones are vulnerable to burglary and have moreover gotten more wanted as the ability to store more information increases. Sabotage occasionally incorporates of the destruction of a business's internet site attempting to cause a lack of confidence to its customers. Info extortion is composed of thievery of a company′s belongings or data as a way to acquire a payment in alternate for returning the information or belongings to its owner. There are a few methods to guard you against a few of those attacks but certainly considered one among the most realistic precautions is consumer carefulness.

Governments, army, firms, banks, medical institutions, and private groups own an excellent deal of personal data about their staff, customers, products, financial analysis, and salaries. Majority of this info is consequently collected, processed, and held on digital computer systems and transmitted throughout networks to different computer systems.

Should private info regarding business customers, finances, or latest products get withinside the arms of the opposition or a black hat hacker, an enterprise and its customers can also additionally go through widespread, irreparable loss, additionally, it's going to cause damage to the company's name. Protecting non-public information is, therefore, an ought to and in numerous instances additionally an ethical and legal demand. A key difficulty for businesses is the calculation of the quantity of cash to be invested from a financial perspective, on info safety. The Gordon-Loeb Model offers a mathematical financial technique for fixing this issue.

For the individual, info safety includes a vital effect on privacy, which is considered in one-of-a-kind methods in numerous cultures.

The discipline of data safety has advanced drastically these days withinside a previous couple of years. There are a few methods of gaining access to the sector as a career. It gives numerous regions for specialization collectively with securing network(s) and allied infrastructure, securing programs and databases, safety testing, information structures auditing, enterprise continuity designing, and virtual forensics.

II. LITERATURE SURVEY

Brute-force Attack "Seeking but Distressing"
Konark Truptiben Dave
2015

A common drawback to web site developers is password guess attack called Brute force attack. A hacker discovers a password by attempting each potential combination of numbers, letters. Some people show carelessness in selecting the user id and password. This could be a risky step to decide on an easy username and password. There's also an issue with the web site developers for selecting username and password. So, what's going to be the answer, which policies are thought-about in selecting username and password and the way are you able to defend against the loot of hackers are given in this paper.

Personal Information in Passwords and Its Security Implications
Mr. Rudresh Gurav, Ms. Leena Dabhade, Mr. Abhilash Kulkarni, Mr. Amar Agarwal, Prof. Rahul Chinchore
2018

Usually, you enter an up-to-date metric known as Coverage to assess the correspondence among passwords and personal information. Then, with the help of our evaluation, we hope to extend the PCFG (Context-Free Probabilistic Grammars) technique to have rich semantics, and we recommend using a personal PCFG to crack the password by making a personalized guess. It shows that personal PCFG can figure out passwords much faster than PCFG, and it increases the possibility of successful cyber-attacks. We usually regard simple operation functions as a unit than the user-selected drive to minimise unnecessary associations connecting personal data with passwords.

GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION
Himika Parmar, Nancy Nainan and Sumaiya Thaseen
2012

In this document, we provide an illustration-based authentication facility that eliminates the requirement for text passcode. When using a commercial prompt texting assistance after the image is verified, the user would be provided with a one-time password (OTP). Users can use this passcode to login to their private accounts.

SQL Injection: Detection and Prevention Techniques
Pooja, Monika
2016

With the rapid increase in the use of the World Wide Web, there is also a hike in the number of threats on web-based applications. Nowadays, SQL injection strikes is believed to be a major problem on the web. It allows unopposed liberty to enter the dataset which leads to the deprivation of probity and secrecy. This article studies and introduces different kinds of SQL injection attacks, and how to determine and ward them off. Our paper might be useful to researchers in choosing an engaging technique for further exploration.

PREVENTION OF SQL INJECTION ATTACK IN WEB APPLICATION WITH HOST LANGUAGE
Surabhi Agrawal, Upendra Singh
2017

Lately, the web is being widely adopted in various sectors. Data security is ensured by the applications as well as their databases that use the Internet while still being able to associate. One of the deadliest attacks i.e., SQLIA robs details of the user from their dataset. The invader can strike SQL commands as well as tamper with the web data by gaining unwarranted entry to critical information. Attackers tend to use queries so as to assail the paramount component in the system security which is the input authenticator. Therefore, it is essential to shut out fatal censure from happening and in order to make that happen and safeguard our dataset, PHP and Java are employed as the main source to avert malicious threats on our requests.

Botnet Detection Technique Using Denial of Service (DDOS) Attack Elliptic Curve Digital Signature (ECDSA) Algorithm
S. Soundharya, K. RaviKumar
2018

They explained three tools: I) Introduce a non-figurative representation for the above attack categories, in which the malware follows standard influx and constantly checks the surrounding for effective sequences. II). As we are aware, inference parameterisation provides congruous estimates for hidden theft that may exist as part of the webwork (that is, coincide with proper conclusion over time). iii) Evaluation of effectiveness in the suggested output scheme in a test bed condition. iv) Elliptic Curve Digital Signature Algorithm (ECDSA) is more recently standardized to reduce the size of digital signatures and supposedly reducing size of digital signatures and cryptographic keys.

Authentication by Encrypted Negative Password
Wenjian Luo,
2019

As part of our structure, a cryptographic hash function (such as SHA-256) is first used to encrypt the simple passcode acquired from the client. Obtain a negative passcode by converting the hashed passcode. Encrypted Negative Ciphers (ENP abbreviations with conformity key rules (such as AES)) and multi-level cipher is used to further upgrade safekeeping. Encrypted hashing and uniform encipher makes it tough to decrypt ENP ciphers.

III. PROPOSED WORK

Existing system:

In existing system, many users regularly choose vulnerable passwords; they have a tendency to reuse identical passwords in special systems; they typically set their passwords with the use of acquainted vocabulary for its comfort to remember. In addition, system issues can also additionally motive password compromises inside the application. Also in existing system, the password or one time password security against intrusion is processed using single encryption algorithm which is easily compromised by intruders having higher end computers. Also, still SQL injection attack is the major frequent vulnerabilities prevailing still in existence losing user confidentiality and trust.

Need for proposed work:

Even nowadays the banks are targeted by the intruder across the globe to compromise the bank server and steal the money, sensitive information's. Few examples are been listed below. Also, still now there is not a single application that invokes security policies addressing all the stages such as user authentication, user pass storage methodology, a defense mechanism against intrusion, user information secure transmission, and storage. Thus, such a kind of application is dreadful as cyber-attacks are getting increased nowadays.

SIM Swap Fraud:

In August 2018, 2 people from Mumbai had been sent to jail for cybercrime. They had been caught doing fraud regarding cash transfers from the accounts of several people via way of means of obtaining their SIM card data via illegitimate methods.

Cyber Attack on Cosmos Bank:

In August 2018, a cyber-attack occurred on the Pune branch of Cosmos Bank. In this cyber-attack, around 94 crore rupees were stolen.

ATM System Hacked in Kolkata:

In July 2018, hackers breached into ATM servers of Canara Bank and stole around 2 million rupees from over 50 people. It is believed that the hackers had access to data of over 300 ATM users across the country

For user authentication, we propose e-mail OTP-based user validation. Also, to eliminate unauthorized access brute force attacks is been addressed. The top web vulnerability attack named SQL injection is addressed by proposing automatic intrusion detection, prevention measures. To eliminate bot-based attacks to the bank server in overloading the requests, we use a captcha-based prevention technique in the negative password, the user provides the plain password which is converted into a hash password by use of cryptographic has function such as SHA 256. Then the acquired hashed password is further changed using symmetric key algorithm such as AES into a negative password. After which the hashed password is changed into a negative password which is then further converted into an Encrypted Negative Password (ENP) with the help of a symmetric-key algorithm e.g., AES. Once user authentication is made secure, secure data transmission to the bank servers has also been addressed. For each file private random key is been generated and assigned. The key is protected from intruders using RC5 based stream encryption algorithm and data owner files are protected using DES encryption algorithm.

The encrypted files are stored in the public cloud storage in a ciphertext format.

Advantage:

1.Security is been addressed in all 3 states such as user authentication, file storage, and data transmission.
2.A new effective approach for securing user passwords differentiating from traditional approaches.
3.Real experimental result-based approach to study the proposed architecture.

Limitation:

1. We have implemented the proposed architecture in localhost as we cannot implement it in real servers.
2. We have used a free e-mail server.
3. The input is limited because we have used only a few exception handling techniques.

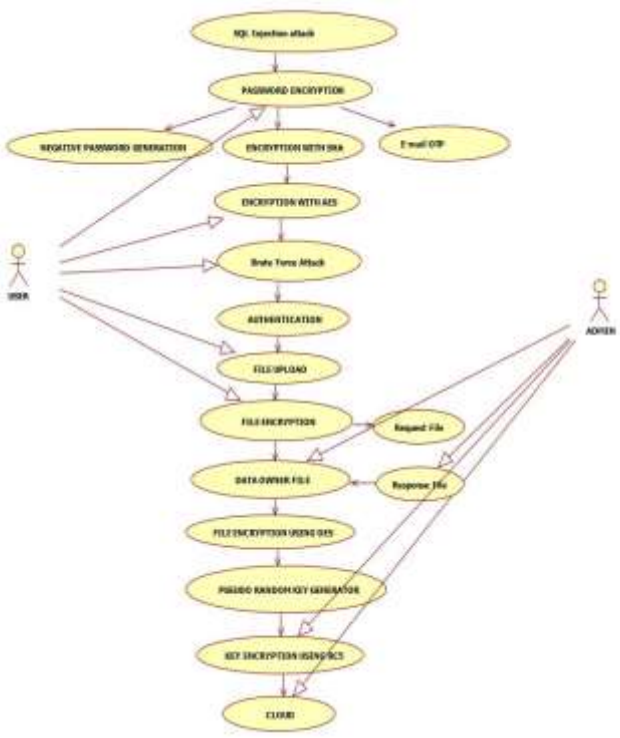


Figure 1: Use Case Diagram

IV. ALGORITHMS

Negative password generation

Pseudocode:

a hashed password hashP;
a negative password np
Output: true or false
1: m ← LENGTH (hashP)
2: for i ← 1 to m with stepsize of 1 do
3: if NUMBEROFSP(npi) 6= i then
4: return false
5: end if
6: end for
7: for i ← 1 to m with stepsize of 1 do
8: if NUMBEROFSP(npi) 6= 1 then
9: return false
10: end if
11: k ← INDEXOFSP(npi)
12: x[k] ←¬TOBIT(npi[k])
13: for j ← i + 1 to m with stepsize of 1 do
14: if npj[k] 6= TOSYMBOL(x[k]) then
15: return false
16: end if
17: npj[k] ←'*'
18: end for
19: end for
20: if x = hashP then
21: return true
22: else
23: return false
24: end if

AES:

Algorithm:

Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
End

RC5 ENCRYTION:

Algorithm:

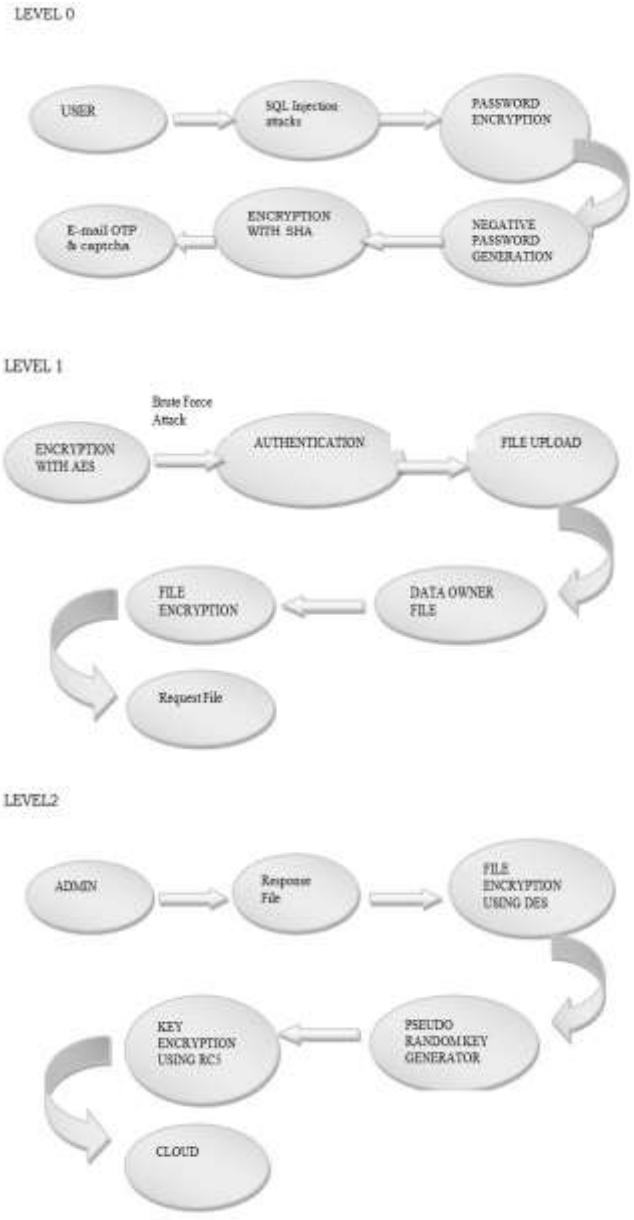
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:
j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j];
It is needed to be observed right here the swapping of the places of the numbers from zero to 255 (each of which

happens once) in the state table. The state table values are given. Once the initialization process is on the verge of completion, the operation process may be summed up as shown by the given pseudo code;

```
i = j = 0;
for (k = 0 to N-1) {
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
swap S[i] and S[j];
pr = S[ (S[i] + S[j]) mod 256]
output M[k] XOR pr }
```

Where M[0..N-1] is the input message consisting of N bits.

V. MODULES & METHODOLOGY



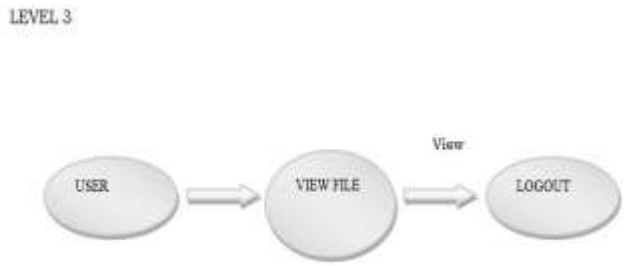


Figure 2: Data Flow Diagram

1. SECURE AUTHENTICATION MODULE:

Negative Password:

Cryptographic hash function generation using SHA-256

The SHA-256 compression function runs on a 512-bit message block and a 256- bit intermediate hash value. It is an essential 256-bit block cipher algorithm that encrypts the following hash value with the use of the message block as a key. Hence there are 2 primary components to give an explanation for: 1 .the SHA-256 compression feature, and 2.the SHA-256 message schedule.

Negative password generation

In our structure, first, the obtained plain password from a customer is hashed using a cryptographic hash function (e.g., SHA-256). Then the hashed password is converted and we acquire the negative password. Finally, with the help of a symmetric key algorithm such as AES, the negative password is encrypted.

Encryption Algorithm – Advanced Encryption Standard:

The Advanced Encryption Standard (AES), regarded to as Rijndael (its unique name), offers a distinctiveness for the encryption of data and information. In 2001, It was set up by the U.S. National Institute of Standards and Technology (NIST).

Two Belgian cryptographers, Joan Daemen and Vincent Rijmen created the AES algorithm. It is a part of the Rijndael cipher. Rijndael includes a set of ciphers with several blocks and different key sizes.

AES runs on a four-by-four column-major order matrix of bytes, regarded as the state, while a few versions or variations of Rijndael have large block length as well have extra columns in the state. Almost all AES calculations are performed in a unique finite field

AES includes many rounds of many procedure steps that embrace replacement, exchange, and adding to the input plaintext and rework it into the ultimate result of ciphertext.

E-mail OTP:

The Email OTP authentication method sends a one-time password (OTP) to the user's email id. The users are validated or authorized through e-mail one-step password authorization.

2. SQL INJECTION MODULE:

SQL Authentication bypass:

A clear SQL injection strike might be able to recondition, switch or destroy the details kept inside the internal dataset, scrutinize sensitive details in addition to performing management operations over the dataset, like shutting down DBMS. As an instance:
Initial Query: Select * from login where User_id='ram'; and password='123'; Insinuated Query: select from login where user_id='' OR 1=1; /'and password='*/-';
As part of the given query, 1 is equal to 1 has been established that is always correct and the remaining portion is accepted and checked like a remark. The assailant gets the entry to the dataset once the request is carried out.

Timing Attack:

As part of this particular theft, the assailant notices the lag in reaction in dataset and gather the required details when gets the chance. This type of strike has similarity with blind injection. The attacker might be able to compute the time required to load a web page as well as verify whether the operator's input is correct. If-Then declaration infuses the query with the help operator. WAITFORE can use keywords to remove the particular time lag in reaction from dataset. As an e.g.:
Declare@ varchar (7000) select @ = db_nameO if (ascii (substring@, 1, 1)) & (power (2, 0)) > 0 waitfore delay '0:0:5';
In case first bit in first byte of the dataset name is 1, then the dataset will be paused for 5 seconds. A setback in inserted code might be encountered when it comes to the feedback duration in case circumstances are suitable.

Prevention technique

Pre-assembled declaration will be used by us to get rid of this in Java.

A. Using prepared statement

In case following statements can be employed

prepared Statement= 'SELECT * FROM emp_table WHERE username = ?'; preparedStatement.setString(1, valid);

It's the way we can be safeguarded from hackers and they will not be able to have access to backend where our details might be stored. The fact that the consumer code is displayed as the material in the specification and won't be as part of the SQL directive, is what the prepared declaration is built upon. However, there may be restrictions on the prepared statements executed in the application. Our query might be vulnerable to SQL strike if we don't write SQL instructions with the help of concatenating 2 strings.

B. Using callable Statement

The callable statement, we will conjointly forestall our query from hackers to retrieve data from our database. It's known as a Public interface callable Statement extends Prepared Statement. The API of java consists an SQL Escape command that permits all the collected process to be referred to as in a standard way for all RDBMS. And this format is employed as the syntax of 1 parameter.

3. ENCRYPTION MODULE:

RC5 Encryption:

The RC5 encryption is a brisk, symmetric block cipher fit for hardware or software application. A unique attribute of RC5 is that the significant usage of information -dependent rotations. RC5 incorporates a variable-length secret key, giving flexibility in its security level. The algorithm is often broken into 2 stages: initialization, and functioning.
The initialization includes a, phase where 256-bit state table is present, S is overcrowded by usage of the key, K which is used as a seed. The state table is built up, it is then persuaded to be changed in a regular pattern as encryption of information occurs.

DES Encryption:

DES algorithm is a block cipher algorithm which encrypts information in block of size sixty-four bit each. A sixty-four-bit plain text is then inputted in the algorithm which led to production of sixty-four bits of ciphertext as output. It's a symmetric-key algorithm, it employs an equivalent key in each encrypting and decrypting the info.

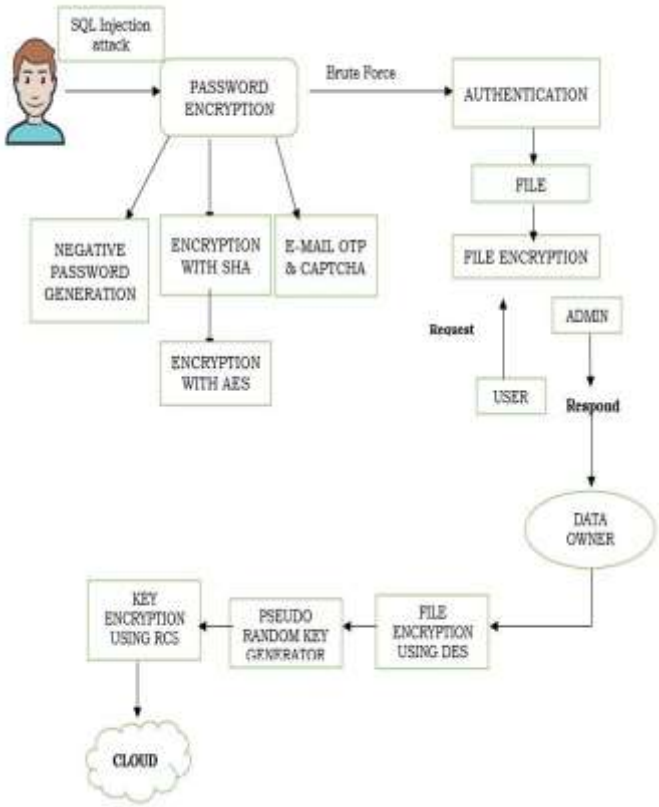


Figure 3: Architecture Diagram

VI. RESULTS DISCUSSION

As motivated towards security in a web application, analyzed security concerns and addressed them in this project study. In this, we have used a hybrid model for rendering security concerns at user authentication, data transmission, file storage stages. For experimental analysis, we have used java programming language with JSP pages for the frontend and MySQL for the backend. The user authentication is secured from unauthorized access by a one-time password, a prevention measure against passwords is stored using a new approach differentiating from the traditional approach through the negative password technique. The data transmission is made secure using an encryption algorithm.

VII. CONCLUSION

In our model, we propose a secure banking application invoking user authentication, secure information storage, addressing the top two web vulnerabilities, and secure data transmission. In this project end to end, the flow of the project is been analyzed on the security aspect and addressed. Despite the traditional approach, we use a unique password protection scheme known ENP. It is then provided a password authentication procedure/structure which is asked on the ENP. Coming over to the end, we analyzed and provided security for passwords and data using cryptographic techniques. Integrating all the aspects into a single application could render complete security gaining end-user trust and confidentiality.

REFERENCES

[1] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipfs law in passwords," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 11, pp. 2776–2791, Nov. 2017.
[2] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, "Targeted online password guessing: An underestimated threat," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 1242–1254.
[3] M. V. Pawar and J. Anuradha, "Network security and types of attacks in network," Procedia Comput. Sci., vol. 48, pp. 503–506, 2015.
[4] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," Comput. Secur., vol. 61, pp. 130–141, 2016.
[5] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, and L. Flynn, "Common sense guide to mitigating insider threats 4th edition," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2012-TR-012, 2012.
[6] J. U. Mills, S. M. F. Stuban, and J. Dever, "Predict insider threats using human behaviors," IEEE Eng. Manage. Rev., vol. 45, no. 1, pp. 39–48, Jan.–Mar. 2017.
[7] D. L. Costa, M. J. Albrethsen, and M. L. Collins, "Insider threat indicator ontology," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2016-TR-007, 2016.
[8] CERT Insider Threat Team, "Unintentional insider threats: A review of phishing and malware incidents by economic sector," Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2014-TN-007, 2014.
[9] C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, "Aspects of insider threats," in Insider Threats in Cyber Security. New York, NY, USA: Springer-Verlag, 2010, pp. 1–15.
[10] D. S. Wall, "Enemies Within: Redefining the insider threat in organizational security policy," Secur. J., vol. 26, no. 2, pp. 107–124, 2013.
[11] L. Liu, O. de Vel, Q.-L. Han, J. Zhang, and Y. Xiang, "Detecting and preventing cyber insider threats: A survey," IEEE Commun. Surveys Tuts., vol. 20, no. 2, pp. 1397–1417, Apr.–Jun. 2018.
[12] M. Turkanovi´c and G. Polanˇciˇc, "On the security of certain e-communication types: Risks, user awareness, and recommendations," J. Inf. Secur. Appl., vol. 18, no. 4, pp. 193–205, 2013.
[13] J. Rene Beulah, C. Pretty Diana Cyril, S. Geetha and D. Shiny Irene, "Towards Improved Detection of Intrusions with Constraint-Based Clustering (CBC)", International Journal of Computer Networks and Applications, vol. 8, No. 1, 2021.
[14] J. Rene Beulah and D. Shalini Punithavathani, "An Efficient Mixed Attribute Outlier Detection Method for Identifying Network Intrusions", International Journal of Information Security and Privacy, Vol. 14, No. 3, 2020.