iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39355

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

Scanning Hybrid Transaction Algorithm for Secure Financial Transactions

Divyansh Joshi[1], Mahak Jain[2]
[1, 2]*Dept. of Computer Science Engg., Shri G. S. Institute of Technology & Science, Indore India*

Abstract: ***Identity theft is a frightening and often very serious concern to everyone. A novel risk-mitigation algorithm, the Hybrid Transaction Algorithm, is given in an effort to provide individuals with peace of mind (HTA). With the random codes, the proposed HTA aims to implement two-factor authentication. This kind of user authentication has been generally recognized, and many businesses have begun to employ it as a security feature. This may be used to identify people and provide a secure method of buying products online. The suggested method involves using mobile devices to log into card accounts using an application in order to examine the randomly generated code. This is then entered when required on an online retailer's website in order to verify the person making the transaction. This reduces the chance of an unauthorized user using someone else's details to make fraudulent transactions. Identity thieves cannot use stolen card information to make transactions unless they have a valid code. This, in turn, protects both the customer and the credit card companies, who may be financially affected. We give one case study to demonstrate the security of our methodology in order to better understand how it may safeguard someone from having a stolen credit card used.***

Keywords: ***Two-Factor Authentication; Hybrid Transaction Algorithm (HTA); AES Encryption; SHA–256.***

I. INTRODUCTION

An online transaction is an activity that occurs from one computer to another in the form of a request and answer. The server responds to user queries instantly. The user also isn't present physically in front of the server; instead, the user connects with the server through a network connection. As a result, the user must be authenticated in order for the server to fulfill the particular user request.

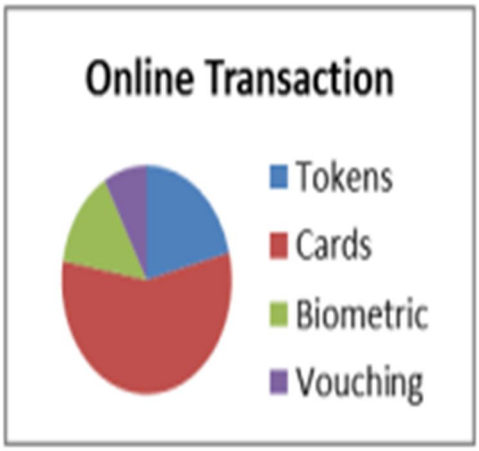


Figure 1: Online Transaction Authentication Methods in Use.

Authentication is the process of granting identification to those working in a company. In the banking industry, for example, banks must identify account holders using a login identification and password. Each transaction made by a consumer should be validated and password secured; all other online transactions, such as shopping, investing, and so on, come to a stop with a banking transaction. Financial data is also of particular importance to intruders or opponents. They attempt to steal the user id and password. There are several sorts of attackers who attempt to hack various objects. Consider user personal information, credit card information, passwords, and so forth. Authentication is based on four elements.

• Something the user understands (Knowledge factor) • Something the user owns (Ownership factor) • Something the user is (Inherence factor) (Mobility factor)

These factors [1] may be used alone for authentication or in combination with others. As a single factor authentication, it is readily hacked; but, when more than one element is added, cracking the authentication system becomes more difficult. As a result, it may give additional security.

The account holder may simply access the account without revealing his or her identify in a face-to-face transaction. However, in online transactions, the account holder must demonstrate that he is the owner of the account and that he is the only one doing the activity. This is an unbeatable challenge in such trades.

II. LITERATURE SURVEY

Breach- D W, PING W, Zhong Chen and CHUN G Ma (2018), in this work Password authentication with a smart card is implemented in remote system to ensure the communication. Here authors used the three-factor authentication. This scheme can achieve mutual authentication, because similar techniques of Bellovin and Merritt's protocol for exchange of key. This work can improve if it will solve the problem of security against offline guessing attacks.

Ding Wang; Ping Wang (2016), the authors proposed various important properties such as New password change; user may have without name and session key agreement. In this proposed system Diffie Hellman public key algorithm is used. In this proposed system password hash function is used to encrypt the password. This system can be used in any security-critical applications, like e-banking, e-commerce and e-health care. Limitation of this work in terms of s where the Human beings memory is inherently limited or stable.

Sk hafizul Islam, Muhammad Khurram Khan and Xiongli(2015),In this work they mentioned about many smart card-based user authentication systems it as be used in wen‟s scheme for user authentication. In this scheme authors concerned about more security and functionalities.

Chenyu Wang and Guoai Xu (2017), In this work distant user authentication is the first step security of online services. In this proposed system they used numerous distant user authentication schemes which is with high ability and efficiency .It can be deployed in various fields such as threat computing, broad casting sensor network. This work is demonstrated with three schemes which is offline dictionary attack, impression attack. This system fails to preserve user anonymity or forward secrecy.

S.k. Hafizul Islam, G.p. Biswas (October 2014), In this project, authors used active ID-based remote user mutual authentication schemes, which implemented using password, smartcard .In this work Diffie-Hellman problem is used. Authors used several ID-based distant user mutual authentication .It has been designed based on one –way hash function and public key cryptography. This work solves the problem of unprotected to password guessing attack and denial of service attack.

Dolev D, Yao A, in this work authors are providing security for the network with the help of public key encryption. In this work new lightweight key management protocol is implemented which allows the constrained node in 6loWPAN Network to transmit captured data to internet host insecure channel. It is more suitable for Protects data integrity and availability.

Shuhua Wu, Yue Fei Zhu, Quion pu(28 April 2011), In this anonymous user authentication is used. Authors used a client to remember a memorable smartcard, where the smartcard stores the secret key. Secret key is issued by the server. In this work, a list of some applications are explained such as online banking, remote host login, activation of security devices , access control of restricted vaults. In this, it mainly relies on the EC computational Diffie-Hellman (ECCDH) assumption. This protocol is used in which provide the secure mechanism in the random model of oracle.

Hsieh-technique Leu's and Wang's PSCAV scheme are utilized for security-critical applications in this paper by Y. G. Wang (2012). The attacker may watch the communication channels and record messages, as well as intercept messages transmitted between the two parties.

Chu-Hsing Lin, Yi-Shing Yeh, Shih-Pei Chien, Chen-Yu Lee, and Hung-Sheng Chien are Chu-Hsing Lin, Yi-Shing Yeh, Shih-Pei Chien, and Chen-Yu Lee (2011), The SHA algorithm is utilized to address the distance issue in this paper (LHV). In today's encryption system, the hash function is quite significant. It's commonly utilized in a variety of applications for password, security protocol, and digital signature protection. In this study, the mathematical procedure cannot be described and sent to the registered user to authenticate their account credentials.

Suleyman Kardas, Ziya Alper genc, Mehmet Sabir kiraz (2017), The authors of this paper discussed the honeywords system, which is utilized as a password breach detection tool. The authors employed one method in this study, which incorporates an extra secure server named "honeychecker." They utilized offline brute-force and dictionary attacks in this case.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

III. DIFFERENT ATTACKS

There are general 25 different forms of attacks while performing cards transaction. These multiple assaults can be divided into four categories: User to root (U2R) attack, Remote to local (R2L) attack, and Probes attacks are all examples of denial of service (DOS) attacks. **Table 1** illustrates of attacks falling into four major attacks.

Table 1: Various Types of Attacks Categories into Four major Attack

Denial of service Attacks	Back, land, Neptune, pod, smurf, teardrop, DoS SlowHTTPTest, DoS Slowloris, Heartbleed Attack	NEW ATTACKS ADDED & PREDICTION IN PROPOSED WORK
User to Root Attacks	Butter_overflow, loadmodule, Perl, rootkit	Port, Scan, Bot, Brute Force, Mail, Bomb, DDOS, Apache 2, DOS, Golden Eya, Phishing
Remote to Local Attacks	Ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster	
Probes	Satan, ipsweep, nmap, portsweep	

1) *Denial of Service (DoS):* In DoS assault, the programmer or interloper sends numerous solicitations that make a server or memory assets too occupied to even consider serving genuine systems administration demands and consequently denying clients' entrance to a machine. There are many attacks that come under DoS.

a) *DOS Back Attack:* DOS Back Attack is a DOS class. It's launched against an Apache Web server that's being inundated with requests with a lot of front-slash (/) characters in the URL description.

b) *Neptune Attack:* Neptune Attack is part of the DOS class. It is possible that transmitting an exchange control convention (TCP) packet signalling the establishment of a TCP connection would cause memory assets to become unusually full, resulting in an unfortunate death. This bundle is part of a three-way handshake that two hosts employ to establish a TCP connection. The unfortunate victim is unable to complete the handshake because to the faked source address, but has distributed some framework memory for this connection. The affected individual finally runs out of memory resources after sending a large number of these bundles.

c) *Pod Attack:* A ping of death occurs when an attacker sends a ping packet greater than 65,535 bytes (normally 64 bytes). A ping heap of this size is forbidden to send, however a package of this size may be sent if it is partitioned. During this attack, a cushion flood occurs, causing the victim's computer to crash.

d) *Smurf Attack:* A huge number of Internet Control Message Protocol (ICMP) bundles with the supposed injured individual's mimicked source Internet Protocol (IP) are sent to the system to use an IP Broadcast address. As a consequence, all hosts in the sector are connected to react to the ICMP request, resulting in the PC of a valid traffic victim. For example, if a network has n hosts connected to it, an attacker might transmit a single packet to the network and compel all of them to send the victim n secure and timely.

e) *Teardrop Attack:* In a teardrop attack, the attacker's IP inserts a jumbled offset value in subsequent fragments, causing the receiving system to crash if it doesn't know what to do.
f) *DoS Slowloris Assault:* The DoS Slowloris assault is scheduled for Wednesday, which matches prior DoS attacks in the CICIDS2017 dataset. The purpose of this attack is to deplete the resources on the victim's device, preventing legitimate users from receiving service.
g) *DoS SlowHTTPTest Attack:* The DoS SlowHTTPTest is executed every Wednesday, and the results are correlated with other DoS attacks in the CICIDS2017 dataset. This attack takes use of TCP's windowing features, wasting resources on the vulnerable server and preventing legitimate users from accessing it.
h) *Heartbleed Attack:* This attack makes use of Heartleech, a Heartbleed exploit tool built in the C programming language. According to reports in the CICIDS2017 dataset, this assault occurs on Wednesday afternoon.

2) *Client to Root Attacks (U2R):* In this harmful untolerable attack, the programmer starts off on the PC with a typical client record and endeavors to abuse vulnerabilities in the PC so as to increase predominant client benefits.
3) *Remote to User Attacks (R2L):* In this harmful untolerable attack, a client sends packets to a gadget over the PC organize, which he/she doesn't have any entrance to, so as to uncover the gadget vulnerabilities and endeavor benefits which a typical client would have on the system.
a) *Guess_Passwd Attack:* The Guess_passwd attack belongs to the R2L class. The Guess_passwd attack involves the intruder constantly guessing potential passwords in order to obtain access to a user's account. Any service that requires a password to enter may be a priority for an attack..

- Probing: In this case, a hacker checks a computer or network infrastructure for bugs that can be used later to breach the system.

b) *Ipsweep Attack:* Probe class contains the IPSweep strike. In a monitoring sweep, the IPSweep attack decides which hosts are listening on the network. It specifies the operating host and its service types, and then attackers will use the details to stage attacks and look for compromised computers.

IV. EXISTING PROBLEM

According to the report, current work focuses on security and developing a model that includes several functions for data processing and transaction processing.

The following are some of the limitations that may be overcome:

1) The present algorithm design does not enable Boolean queries, therefore the rapid format of inquiry is not supported, which is a shortcoming in current work that may be addressed in the suggested study.
2) The participation of multiple components and the number of individual algorithms increases the architecture's complexity, which may result in a high computational cost. This may make the suggested design easier to understand.
3) A 256-bit group order safety is presented, which may enhance up to a 160-bit key and so produce a strong key.
4) High computation costs may cause a common mid-level business to fail if it is in need of improvement.
5) There are further attack resilience models that may be offered.

V. PROPOSED ALGORITHM- AES ENCRYPTION ALGORITHM

The Advanced Encryption Standard (AES) is one method of data security that encrypts and decrypts data. The user then inputs a key that is encrypted using the SHA-256 algorithm to protect the file's contents when the file is loaded into the software. To get around the current issue formulation. The model will be approached in the following manner.

1) A secure search technique that can also do Boolean searches over a secure proxy data server.
2) A method of encryption that would be both quick and efficient when compared to proxy re-encryption and encryption. The AES ENCRYPTION ALGORITHM may be utilized to improve the existing security method's performance.
3) Several conjunctive phrases and data searching utilizing the Boolean query method are employed in addition to the current scenario.
4) A reduced model with fewer components, as well as a high-security and searching approach, and a word connection building strategy, will be shown.
5) Finally, a SaaS solution will be supplied, with the aforementioned security and multi-keyword search functionality.

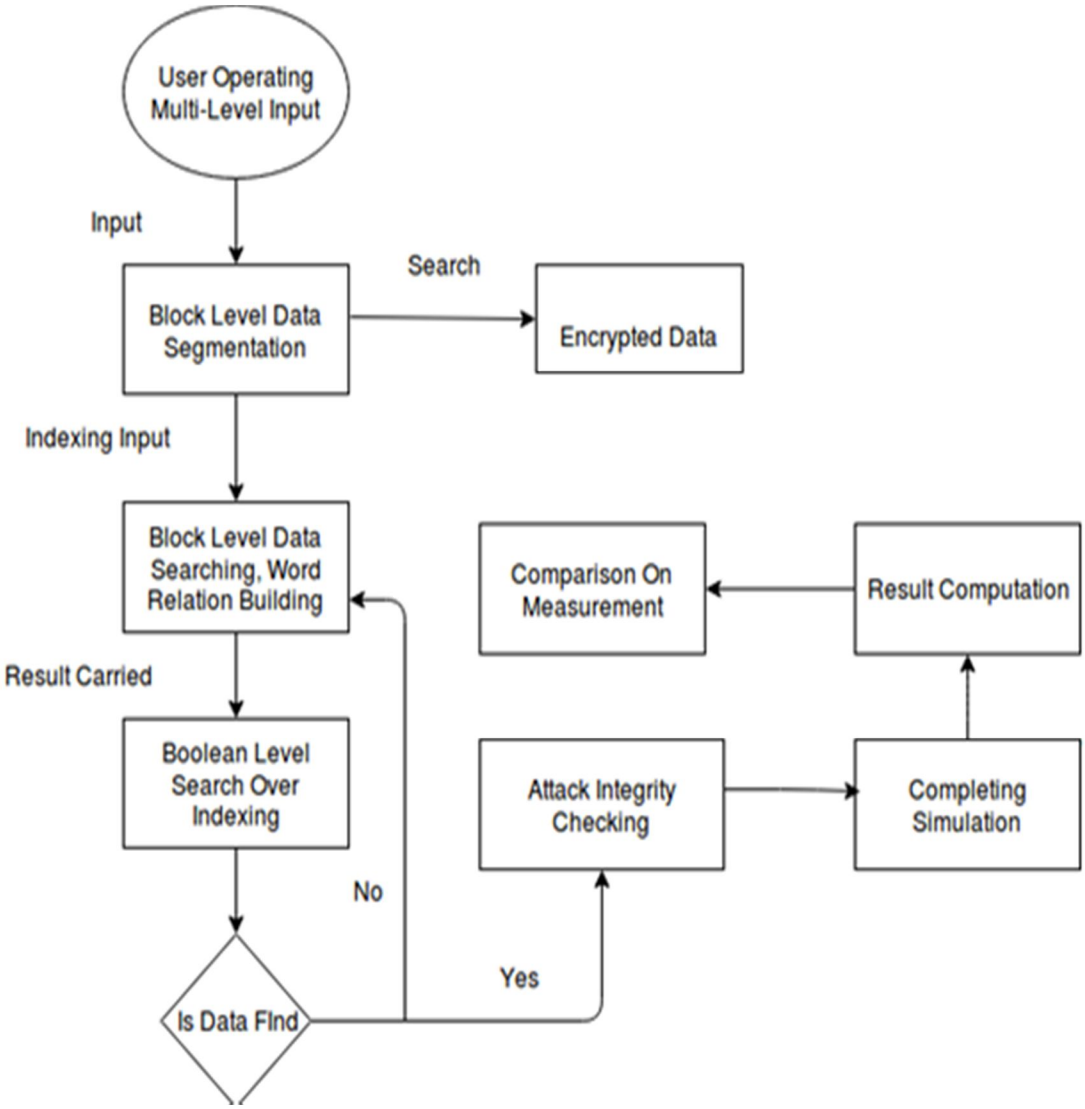


Figure 2: Flow architecture of given proposed solution.

The flow graphic above describes how the suggested algorithm works.

Figure 2 shows a solution that explains-

a) *Step 1:* The component specified multiple level of word search and storage is shown in the multiple solution entity diagram. Initially, data is saved on the server, and then it is stored in an encrypted manner in the database.

b) *Step 2:* On the basis of the input received from the cloud server, block level data segmentation will be performed, and the data will be stored across its architecture in encrypted storage.

c) *Stage 3:* In this step, block level data searching and word relation construction are combined. The encrypted data is then subjected to a conjunctive keyword search.

d) *Phase 4:* This step validates the solution's searching capabilities, as well as providing a Boolean search of stored data with an effective data query output solution.

e) *Step 5:* If relevant data is found, it will proceed to attack integrity verification; otherwise, it will revert to block level data scanning.

f) *Step 6:* Finally, the simulation will be completed, taking into account compute time, throughput, and cost.

g) *Step 7:* The execution demonstrates that the suggested solution is superior to the standard data storage and access methods.

A. Algorithm Execution (Pseudo Code)

The main goal of this Pseudo code algorithm approach is to remove the user from the execution process. The number of inputs, the processing of the method, and the finding of the answer are all detailed.

Input may take the form of a database, encrypted data Edi, multi-keyword input, or a Boolean query.

Output might include things like search results, relevant data, CPU use, and throughput.

```
Input: Database, Encrypted data Edi, multi keyword input,
Boolean query
Output: Search output, Relevant Data, computation usage,
throughput
Steps:
Begin[
Initializing library frameworksetup();
Processing AES encrypted data storage;
AESStore()
{
Selection of data;
KeyGen();
Encrypt(Key,Data);
Keyword Selection;
EncUpload(Key,Data,Keyword,Timed Parameter);
}
For each keyword (keyword processing)
{
Finding word relevance;
Boolean breakup();
}
Access indexing from AES data with SHA-256();
Word relation building;
Boolean search function ()
{
Query working with 0 or 1;
}
Finding keyword score;
Data matching ();
Return;
Timed parameter monitoring ();
Data integrity verification ()
{
Token searching ();
Token verification ();
}
Return verResult;
Compute utilization ();
Computation outcomes;
End];
```

The pseudo code provided for algorithm execution is a simplified version of the functions utilized throughout the execution. The participant's data storage functions, their method, and finally their interaction with the search mechanism are all shown. Furthermore, the feature allows users to search for data in secured cloud storage.

B. Advantages Of Proposed Algorithm

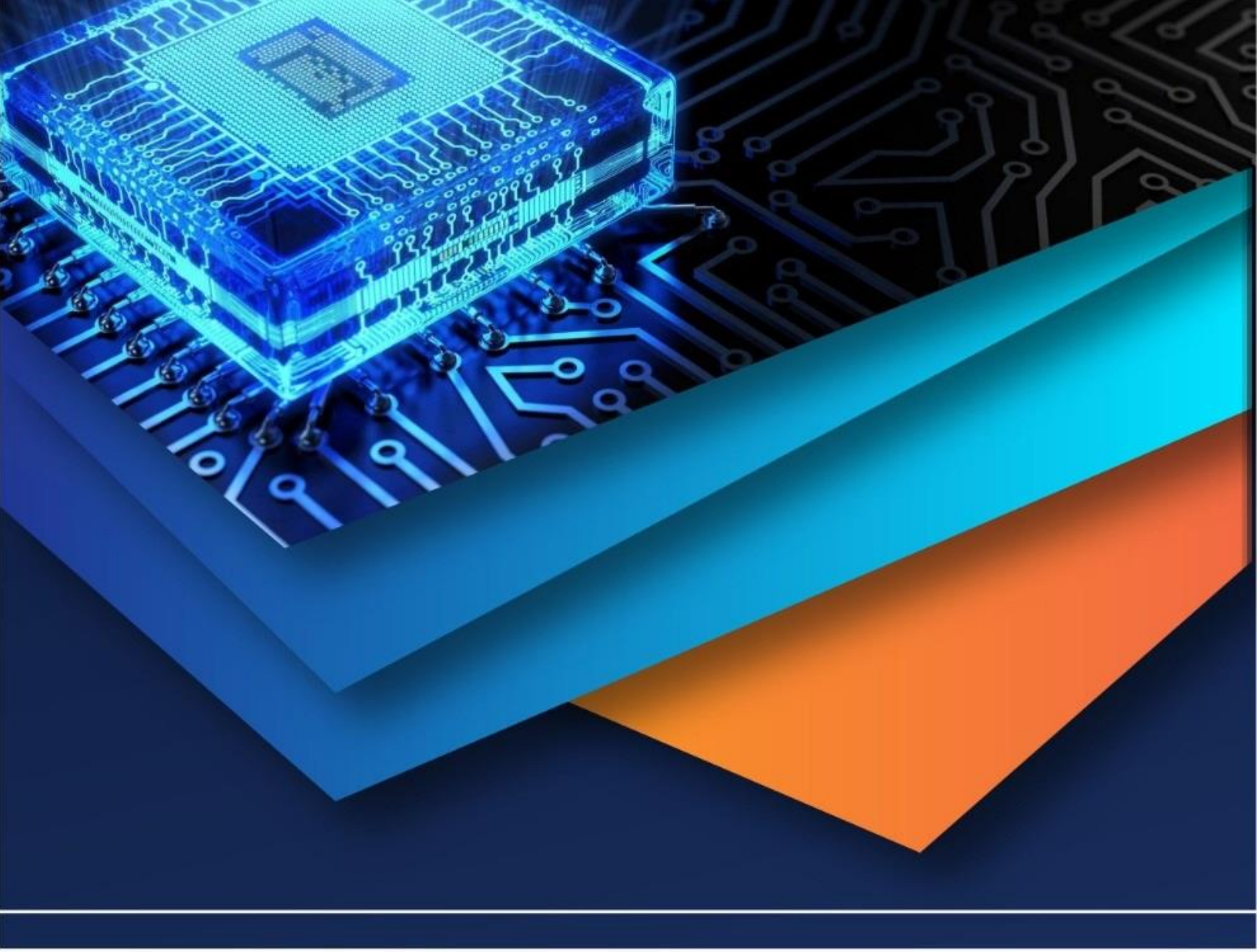
1) A security approach algorithm which can generate potential key in less computation time and cost.
2) Performing an efficient storage of data and further working Conjunctive keyword searching upon performing relation between the keywords.
3) Providing a proper access control, searching and posting the data as per requirement in a secure media.
4) To provide a system this can help in resisting the searching attack such as keyword guessing attacks and sql injection.
5) Multi-party access and its control over the data as per rights usage provide need to be performed in proposed model.

VI. CONCLUSION AND FUTURE SCOPE OF WORK

The goal of this research is to create a highly secure environment for internet transactions. To address this issue, the authors recommend that mobile phones be used as the primary source of authentication. If the OTP is not entered on the approved hardware device, which can be identified by its unique ID, the transaction will fail. The proposed programme should be hard-coded in the mobile device and never changed. In the future, researchers will be concerned about protecting the generated OTP from man-in-the-middle attacks and other types of attacks. An additional security layer or encrypted communications techniques may be used to protect communication between both the consumer and the financial institution server.

REFERENCES

[1] D. Wang, P. Wang, Two birds with one stone: Two-factor authentication with security beyond conventional bound, IEEE transactions on dependable and secure computing, 15(4), 2018, 708-722.
[2] Z. A. Genc, S. Kardaş, M.S. Kiraz, Examination of a new defense mechanism: Honey words, IFIP International Conference on Information Security Theory and Practice, 2017, 130-139.
[3] S. H. Islam, M. K. Khan, X. Li, Security analysis and improvement of „a more secure anonymous user authentication scheme for the integrated EPR information system, PloS one, 10(8), 2015, 1-19.
[4] C. H. Lin, Y. S. Yeh, S. P. Chien, C. Y. Lee, H. S. Chien, Generalized secure hash algorithm: SHA-X, EUROCON-International Conference on Computer as a Tool (EUROCON), 2011, 1-4.
[5] D. Wang, C. G. Ma, P. Wang, Z. Chen, Robust smart card based password authentication scheme against a smart card security breach, Cryptology ePrint Archive, (439) 2012, 1-35.
[6] C. Wang, G. Xu, Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card, Security and Communication Networks, 2017, 1-15.
[7] D. Dolev, A. Yao, On the security of public key protocols. IEEE Transactions on information theory, 29(2), 1983, 198-208.
[8] K. Hussain, N.Z. Jhanjhi, H. Mati-ur-Rahman, J. Hussain, M. H. Islam, Using a Systematic Framework to Critically Analyze Proposed Smart Card Based Two Factor Authentication Schemes, Journal of King Saud University-Computer and Information Sciences, 2019, 1-9.
[9] M. Sbeiti, C. Wietfeld, One stone two birds: On the security and routing in wireless mesh networks, IEEE wireless communications and networking conference (WCNC), 2014, 2486-2491.
[10] S. Manishankar, P.R. Ranjitha T.M. Kumar, Energy efficient data aggregation in sensor network using multiple sink data node, IEEE International Conference on Communication and Signal Processing (ICCSP), 2017, 0448-0452.
[11] A. Santosh, A.R. Pillai, A protocol for efficient utilization of energy in wireless sensor network, Science Publishing Corporation, 7 (3.3), 2018, 82-86.
[12] B.S. Kumar, A. Nair, V.R. Raj, Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images, IEEE International Conference on Communication and Signal Processing (ICCSP), 2017, 1057-1060.
[13] B.S. Kumar, V.R. Raj, A. Nair, Comparative study on AES and RSA algorithm for medical images. International Conference on Communication and Signal Processing (ICCSP), 2017, 0501-0504.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY