iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

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 :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

An Efficient Analysis to Avoid Shadow Attack on Password Reuse

Kiruba. J. Amanda[1], Dr. A. J. Deepa[2]
[1]*M. E. Ponjesly College of Engineering, India*
[2] *M.E, Ph. D Professor, Department of CSE. Ponjesly College of Engineering, India*

Abstract: ***Nowadays people do their transaction in online. This will help to reduce time. People can create different accounts to register their user name and password. The password select by this people is not well secured. The password create by those people will remain the same. It will cause insecure concept for the data. The attack that cause in this kind of scenario is the shadow attack. This attack is a simple guess of the intruders will lead to the insecurity in networking. The problem can be studied and overcome in this project by implementing to successive scenarios in this paper. One is Intra Site Password Reuse (ISPR) and the next one is Cross Site Password Reuse (CSPR). This will allow the user to select the password and they are allowed to reuse the password without causing the shadow attack. The data base design and the preprocessing step will increase the security in this kind of area. Thus the user can ultimately select the password with the same sequence. It is a user friendly application model for store the password with high accuracy and security***
Index Terms: Password, Security, CSPR, ISPR, Shadow attack

I. INTRODUCTION

Recently in china there was a large disaster occur due the manual and technical fault. The famous website which was storing the numerous number of people data was publicly leaked. Thus the secure password is now available in public. The intruders, hackers, spoofers are pretty much used the leaked password. Thus many people suffer a lot due to this disaster. This is the main thing that the most of the people is not willing to store their data in a third party service provider. The main cause of this problem is due to the technical problem. The main drawback that suffer in this scenario is most of the people who used to maintain their data is protected by the secure password. This can be done by the secure database server by the host. Most of the people who are from different occupation such as Administrator, Business Man, common people government worker maintain their data in cloud to use it in anywhere at any time. There is no limitation so they can store their data is either any one of the site or multi-site. Here the data which is stored by the different criteria of the people is denoted for storing their password in a well encapsulated manner. Thus the data that maintained by the senior citizen is not pretty much evaluated. Thus the security of password is not unique to some of the person. Many times the data that used to provide the password in the insecure way. Thus the same problem is done in the china. Most of the citizens of china is used to store their data in different site or the same site occurred a problem when the data base leaked. The password is publicly taken by the hackers. Then they apply the password in various scenario such as bank account, user details, passbook etc. The misuse of the revealed data is violently affect most of the citizens in china.

Thus in this research the better idea for protecting this password is simply made by the commonly used model. This novel technique is taken from the Levenshtein distance Algorithm [1]. The scientist shows that the password is protected by the simple way. The most of the user who used to store their data in different manner in different type. Those password can be simply made by the novel algorithm technique in this research.

Most of the password is stored in the systematic manner is explained in simple and easiest algorithm. The data which is used to propose the model is based to overcome the shadow attack. And also the user can freely reuse their password at any time anywhere.

II. RELATED WORK

[11] Robert Morris and Ken Thompson, proposed and elaborates the idea about Password Security with deep history evaluation. Here they implemented the UNIX based systematic approach for securing the OS. Here the password is used to maintain a simple data using the Encryption format. The mechanism they used to try to proposed is of simple and ethnic way at which the data can be simply poster and the user needs to select the key for encrypting the file using the required key. Thus the encryption is done while storing in the database. Thus once the user select the password and they enter into the database. In the data base storage inbuilt key provided by the sites was maintained. When the password entered it automatically encrypt the password and the encrypted data stored in the data base. Which it leads to time consuming. When there is additional pattern issuesthe password may get corrupted.

[12] Today's Internet services rely heavily on text-based passwords for user authentication. The pervasiveness of these services coupled with the difficulty of remembering large numbers of secure passwords tempts users to reuse passwords at multiple sites. In this paper, we investigate for the first time how an attacker can leverage a known password from one site to more easily guess that user's password at other sites. We study several hundred thousand leaked passwords from eleven web sites and conduct a user survey on password reuse; we estimate that 43- 51% of users reuse the same password across multiple sites. We further identify a few simple tricks users often employ to transform a basic password between sites which can be used by an attacker to make password guessing vastly easier. We develop the first cross-site password-guessing algorithm, which is able to guess 30% of transformed passwords within 100 attempts compared to just 14% for a standard password-guessing algorithm without cross-site password knowledge.

[13] We evaluate two decades of proposals to replace text passwords for general-purpose user authentication on the web using a broad set of twenty-five usability, deploy ability and security benefits that an ideal scheme might provide. The scope of proposals we survey is also extensive, including password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. Our comprehensive approach leads to key insights about the difficulty of replacing passwords. Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use. We conclude that many academic proposals have failed to gain traction because researchers rarely consider a sufficiently wide range of real-world constraints. Beyond our analysis of current schemes, our framework provides an evaluation methodology and benchmark for future web authentication proposals.

[14] The problem of shadow attack based on password reuse technology overcome by Weili Han, ChenSun, Chenguang Shen, Chang Lei, ean Shen presents combining multiple factors during authentication, a service can provide better assurance of security. However, the users are likely to feel inconvenient, or even discard the service. This paper, therefore, addresses this issue and introduces a novel method, referred to as the Quantified riSk and Benefit adaptive Authentication Factors combination (QSBAF). QSBAF balances the requirements for both security and usability in the authentication of an information system and improves the system's ability to respond quickly to emerging risky events. In QSBAF, the authentication factors can be dynamically combined on the basis of quantified risk, benefit measurements, and combination policies. Furthermore, QSBAF provides an adaptive mechanism, which is driven by history data to justify the measurements of risk and benefit. In this paper, we use the online banking system as a typical scenario to demonstrate the usage of QSBAF. We also implement a prototype of QSBAF to evaluate the performance of its feasibility in real application scenarios.

[15] The problem of shadow attack based on password reuse technology overcome by Jerry Ma, Weining Yang, Min Luo, Ninghui Li presents a probabilistic password model assigns a probability value to each string. Such models are useful for research into understanding what makes users choose more (or less) secure passwords, and for constructing password strength meters and password cracking utilities. Guess number graphs generated from password models are a widely used method in password research. In this paper, we show that probability-threshold graphs have important advantages over guess-number graphs. They are much faster to compute, and at the same time provide information beyond what is feasible in guess-number graphs. We also observe that research in password modeling can benefit from the extensive literature in statistical language modeling. We conduct a systematic evaluation of a large number of probabilistic password models, including Markov models using different normalization and smoothing methods, and found that, among other things, Markov models, when done correctly, perform significantly better than the Probabilistic Context-Free Grammar model proposed, which has been used as the state-of-the-art password model in recent research.

[16] The problem of shadow attack based on password reuse technology overcome by Jay Destories Mentor: ElifYamangil presents many systems use passwords as the primary means of authentication. As the length of a password grows, the search space of possible passwords grows expo- mentally. Despite this, people often fail to create unpredictable passwords. This paper will explore the problem of creating a probabilistic model for describing the distribution of passwords among the set of strings. This will help us gain insight into the relative strength of passwords as well as alternatives to existing methods of password candidate generation for password recovery tools like John the Ripper. This paper will consider methods from the field of natural language processing and evaluate their efficacy in modeling human-generated passwords.

[17] The problem of shadow attack based on password reuse technology overcome by David Silver, Suman Jana, Eric Chen, Collin Jackson and Dan Boneh presents the security of popular password managers and their policies on automatically filling in Web passwords. We examine browser built-in password managers, mobile password managers, and 3rd party managers. We observe

significant differences in auto fill policies among password managers. Several auto fill policies can lead to disastrous consequences where a remote network attacker can extract multiple passwords from the user's password manager without any interaction with the user. We experiment with these attacks and with techniques to enhance the security of password managers. We show that our enhancements can be adopted by existing managers.

III. PROBLEM IDENTIFICATION

In previous mechanism the data that stored in the normal database is not valuable it can be processed and maintain in a simple scheme of which it should be used. The main use of the database is used to protect the data. If any one of the malfunction done in that website is not accurate.

A person can register several accounts on websites. If their registered email addresses are the same, we believe these accounts belong to the same user. That a person may use multiple emails addresses to register multiple accounts, and addition information could be obtained to link these email addresses. *e.g.,* User's corresponding friends may be aware of the linkage or it can be identified by the same email name but different email domain.

A. Disadvantage

1) Anyone can easily reuse their passwords of their multiple accounts

2) By using this method user possible to maintain multiple accounts on same site with same password

B. Architecture of Problem Identification

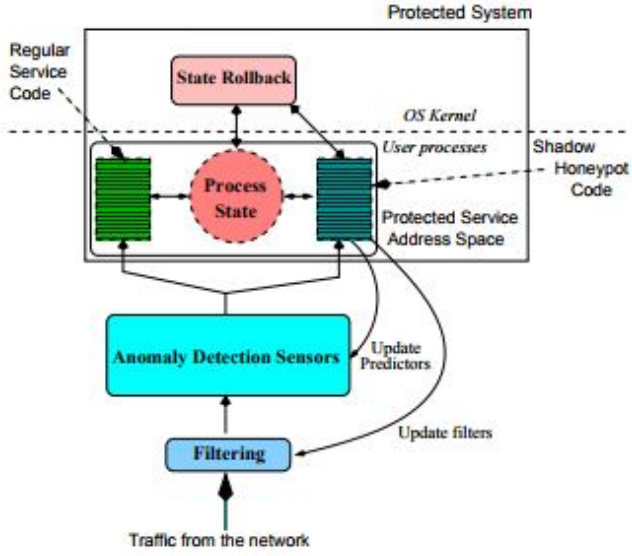


FIGURE 1: Shadow Attack Prevention

The shadow attack prevention is maintained in this module here the data that is used to process for the simple and efficient dual core process maintained using honey pot pattern the honey pot pattern is used to maintain used for simple process. This should be avoided with the mesh related format. Here the anomaly detection taken place using the simple and efficient scheme of performance through which it can be maintained.And the process which the regular service code is maintained and process with the simple and proficient mechanism of data processing. The data processing mechanism of which it can be maintained and regularized in a simple and efficient scheme formatting protocol of which it should be determined. The entire details are maintained in the OS kernel of which it could be forwarded. The main use of the proposed scheme is not valid and it is not processed in the simple scheme of which it should be used.If the shadow detects an actual attack, we notify the filtering component to block further attacks. If no attack is detected, we update the prediction models used by the anomaly detectors. Thus, our system could in fact self-train and fine-tune itself using verifiably bad traffic and known mis-predictions. The Shadow Honey pot architecture is a systems approach to handling network-based attacks, combining filtering, anomaly detection systems and honeypots in a way that exploits the best features of these mechanisms, while shielding their limitations. We focus on transactional applications, i.e., those that handle a series of discrete requests. Our architecture is not limited to server applications, but can be used for client-side applications such as web

browsers, P2P clients, etc. As illustrated in Figure 1, the architecture is composed of three main components: a filtering engine, an array of anomaly detection sensors and the shadow honeypot, which validates the predictions of the anomaly detectors

IV. PROPOSED MODELING

In this research work the existing drawback is overcome by finding the misbehaving user. Managing passwords is still challenging, especially when the number of distinct passwords is large. A user should reuse their passwords in similar accounts, because impossible to remember so many passwords, and input them in correct user interfaces. A user should have stronger security concerns to protect their accounts, especially some high-valued accounts, from the threat of ISPR and CSPR. For example, they should not reuse their passwords of some forum sites in their online banking accounts.

The proposed model is used to identify the prefix mechanism of which it could be used for the simple mechanism of easy view of approach. This mechanism can be implemented and maintained under the simple use of performance through the mechanism of simple architecture model.

A. Proposed architecture modeling

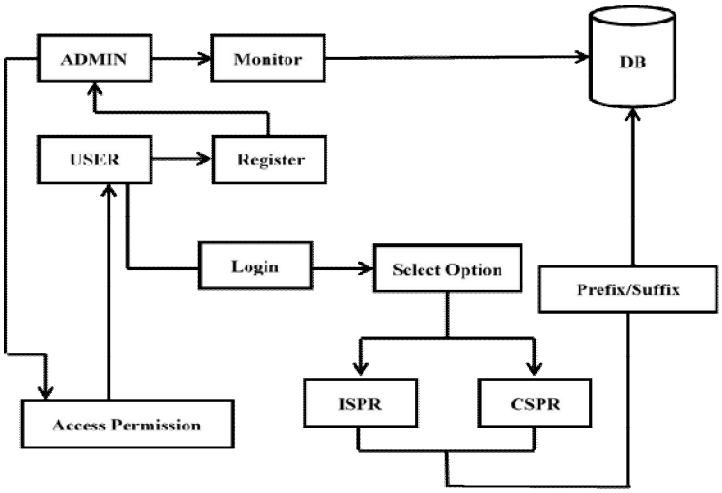


Figure 2: Architecture Of Proposed Modeling

B. Implementation

Implementation is the stage of the project when the theoretical design id 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 constrains on implementation, designing of methods to achieve changeover.

C. Admin Module

The first module in the design is the Admin module. The admin module is used to process under the specification purposes. The methodology purposes are based upon the web based application criteria. Through which the admin can account the behaviors of the user.

D. User Module

The Next module in this work is registration process. This module is designed for the security purposes. The registration module is designed with the modularization purposes. The user needs to register under the administration process.

E. Dataset Design

Dataset design is the next design of module. The modeled purposes are used to avoid the data set leakage in the system. Here the data set is designed with the clustering and hierarchical process. The clustering is the grouping mechanisms were the data are designed with the simple and effective process. The hierarchical model is used to link between the resource and the system .The process usability is used to link between the resource and performance maintenance of the system is used to design. The usage of data set is used to avoid the resource leakage of the user and guarantees the security mechanism.

F. User classification

The next process is the user classification mechanism. The user classification mechanism is designed with the two data set process one is ISPR and another one is CSPR .The ISPR is derived as the Intra site password reuse and the CSPR designed for the cross site password reuse. Thus the performance is used for the simple suffix and prefix model.

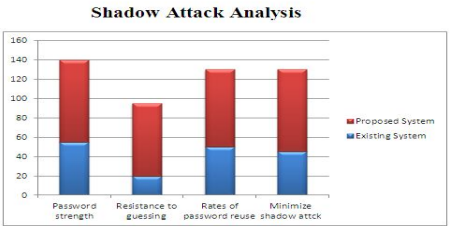
G. Quantitative Analysis

The final module is the Quantitative analysis model .This used to concern the methodology or techniques that can be empirically is used for the simple mechanism. The suffix and prefix model is the simple and efficient performance metrics that is designed in the keyboard side. Thus this trustfully avoids the shadow attack.

V. RESULT AND DISCUSSION

A. Performance analysis

To evaluate shadow attacks, we use the diverse password pairs in D_{csdp} to perform the experiment, and diverse password pairs are distinct passwords of crosssite accounts of the same users. In addition, we use the weaker passwords in thediverse password pairs to guess the stronger ones. This shows the danger of the widely adopted users' behavior: using weaker passwords in low-valued accounts and stronger but similar ones in high-valued accounts.



B. Experiment Setup

The methods being tested include the following.

1) JtR default: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with JtR default rules

2) Jt Runi: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram prefix/suffix rules.

3) JtR bi: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram and bigram prefix/ suffix rules.

4) JtR tri: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram, bigram and trigram rules.

The added prefixes/suffixes are listed and then in the latter three methods, we delete the default prefix/suffix rules pre-installed in JtR. In addition, the patterns double, case transformation and reverse already exist in JtR default rules.

C. Limitations

Quality and number of datasets: Our password datasets are from four Chinese websites. Although Chinese Internet users accounts for a large portion of the entire Internet users, our study mainly reflect the password reuse patterns of Chinese users. Our data pre-processing steps may have caused underestimation of password reuses. Mapping between persons and users: In our research, did not analyze the scenario where a person registered as multiple users on sites using different email addresses, because we do not have enough information to perform this analysis. Although we may merge several accounts with the same complex passwords d to one human user, we cannot apply this method to all accounts in our analysis.

D. Security Suggestions

Managing passwords is still challenging, especially when the number of distinct passwords is large. Florencio et al. even proposed that a user should reusetheir passwords in similar accounts, because they argue that it is impossible for a user to remember so many passwords, and input them in correct user interfaces. We thus suggest:

A user should have stronger security concerns to protect their accounts, especially some high-valued accounts, from the threat of ISPR and CSPR. When a webmaster wants to measure the strength of passwords, he or she should consider the threat of ISPR and CSPR. That is, when a similar website. A password manager could be a good helper to manage a large number of passwords, although some threats or vulnerabilities still exist. In addition, multiple factors should be popular in the nearly future. Then the dynamic combination method of authentication factors might offer more user-friendly experiences

E. Password Reuse Rates Of Different User Groups

This result confirms our hypotheses that users in academic organizations are better educated with web security than common users and tend to use different passwords for accounts in different websites. Another reason may be that users incline to reuse passwords when registering with low-valued or easily replaceable email accounts. Academic emails, however, are difficult to be replaced.On the contrary, it is interesting to find out that users with international email addresses are most likely to reuse their passwords cross-site. Surprisingly, VIP users, those who would pay annual fees for their email addresses, also have a high rate of cross-site password reuses, which is second to I18n users.

Email Category	# of Reuse Accounts	# of All Accounts	Reuse Rate
VIP	7,063	20,442	34.55%
EDU	712	2,725	26.13%
Chinese	614,989	1,970,522	31.21%
I18n	40,164	114,734	35.01%
Total	662,928	2,108,423	31.44%

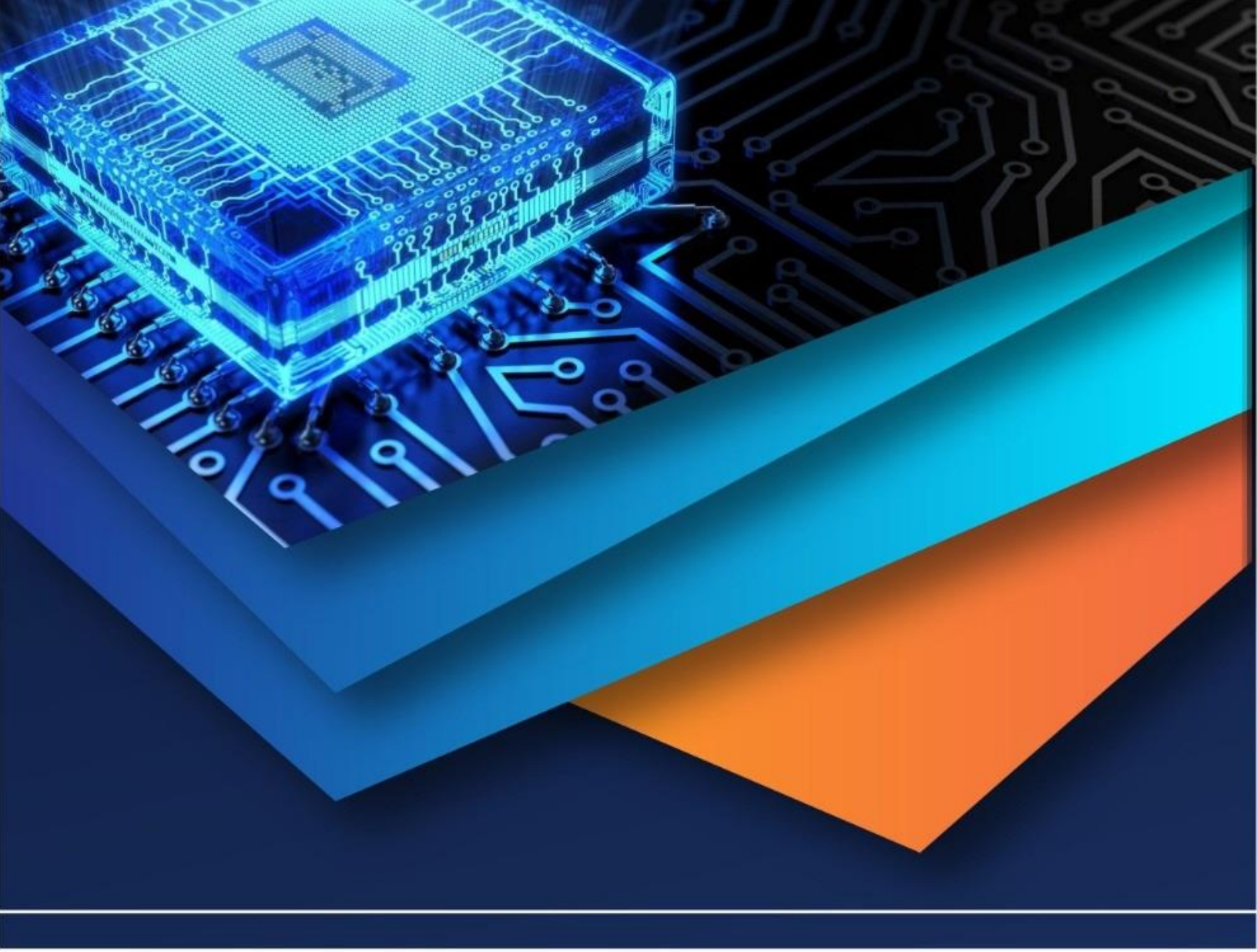
Fig: Reuse Rates of CSPR of Different User Groups

VI. CONCLUSION

The phenomenon of web password reuses (both ISPR and CSPR) utilizing the large password corpora. The quantitative answers shed lights on the serious threat where an adversary may attack an account of a user using the same or similar passwords of his/her other less sensitive accounts. We would study CSPR from both adversaries' and defenders' points of view, leveraging the logs or activities that are available in the public domain. In addition, we will evaluate how the password policies affect CSPR after understanding the policies of these four websites. Last but not the least; we plan to study the impact of single sign-on tools on password reuses

REFERENCES

[1] R. Morris and K. Thompson, "Password security: A case history," Communications of the ACM, vol. 22(11), pp. 594–597, 1979.
[2] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in NDSS'2014, 2014.
[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW'07 Proceedings of the 16th international conferenceon World Wide Web, 2007, pp. 657–666.
[4] CSDN, http://www.csdn.net/company/about.html.
[5] http://help.tianya.cn /about/history/ 2011/06/02 /166666.shtml."
[6] Duduniu, http://baike.baidu.com/view/1557125.htm.
[7] 7k7k, http://www.7k7k.com/html/about.htm.
[8] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in 2012 IEEE Symposium on Security and Privacy (SP), 2012, pp. 538–552
[9] J. Ma, W. Yang, M. Luo, and N. LI, "A study of probabilistic password models," in Proceedings of IEEE Symposium on Security& Privacy, 2014
[10] Z. Li, W. Han, and W. Xu, "A large-scale empirical analysis of Chinese web passwords," in 23rd Usenix Security Symposium. San Diego: USENIX, 2014.
[11] D. Wang, H. Cheng, Q. Gu, and P. Wang, "Understanding passwords of chineseusers:characteristics, security and implications," https://www.researchgate.net/, July 2014.
[12] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy, "Visualizing keyboard pattern passwords," in Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on. IEEE, 2009, pp. 69–73
[13] "Longest common subsequence problem," http://en.wikipedia.org/wiki/Longest common subsequence,May 2014.
[14] J. the Ripper, "John the ripper password cracker," http://www.openwall.com/john/, May 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY