ISSN:0975-9646

Survey for Generating an Ideal Password Authentication Scheme Which Results In Fortification of Transport Layer Security Protocol

Kuljeet Kaur ,Dr. G.Geetha
School of Computer Applications, Lovely Professional University (Phagwara –[PB]. India)

***Abstract*— Fortification of transport layer security protocol is required because whenever there is communication between Client and Server over a public link, then proving an identity becomes quiet complex. When resources are to be accessed from remote systems through public network then identity authentication parameters are the de-facto-standard. Paper elucidates upon various authentication parameters and generates a result that there is need for generating an ideal password authentication scheme. Analysis through a survey is done and outcome is formulated for efficient authentication type for online transactions. Evaluation of security and privacy for online transactions is examined in the paper and overall expectations of the user for e-purchasing, e-banking or e-communication etc is formulated. Complete paper explicates that user needs one more tier of security for complete secure and assured transactions in public network. Analysis is publicized through comparative bar charts in the paper with possibility of acceptance of the user in terms of bearing extra cost for ideal password authentication scheme which will result in fortification of transport layer security protocol.**

***Keywords*: Network Security, Authentication Parameters, Privacy, Fortification, Transport Layer**

I. INTRODUCTION

When there is public link and resources are to be accessed from remote systems then proving an identity becomes quiet complex because there is need of proper access rights with authentication. Various authentication parameters like Password, smart Card, Fingerprint and Pass Phrase are used for proving the identity of Client and Server both. Moreover complete security at the transport layer starts with proof of authentication only and assures the security and information. This paper has analyzed all the identity authentication parameters with a Survey. It was conducted at different locations among the age groups from 20 to 40 years and a result is derived that one additional tier of security is to be assimilated for fortification of transport layer. Mutual authentication would be done in tiers and the survey has examined that user's can bear additional cost also for complete security and assurance of transactions.

Remaining sections of the paper are Section II elaborates upon the features and parameters which were kept for the survey for generating an ideal password authentication scheme, Section III elucidates the analytical representation of parameters of the survey with the help of bar charts, Section IV analyzes the survey results, Section V concludes the paper on the basis of results derived from the survey and Section VI acknowledges the people who has contributed for the smooth conduct of the survey.

II. PARAMETERS FOR SURVEY FOR GENERATING AN IDEAL PASSWORD AUTHENTICATION SCHEME

The identity authentication parameters are required for mutual authentication in the public network. The Survey is conducted for analyzing that transport layer security protocol needs fortification. Ideal password authentication scheme is required for fortification. Following questions were asked from the users in the form of a questionnaire for analysis:

1. Which among the following is the most common and accepted authentication method for online transactions which you generally use?
   (Password, Smart Card, Fingerprint, Pass Phrase)
2. What do you face as the most concerning challenges in online transactions? (Authentication, Security, Usability, None)
3. How secure do you think passwords and tokens are during online transactions?
   (High, Medium, Low, Not Secure)
4. How do you perceive usability of passwords and tokens are during online transactions? (High, Medium, Low, Not Decided)
5. Which of these authentication types would you use for online transactions in future? (Fingerprint, Iris, Location Based, Voice Recognition)
6. How do you evaluate security and privacy in online transactions if fingerprint is used as an authentication type?
   (High, Medium, Low, Not Secure)
7. What are your expectations to secure your transactions while using online mode (either for e-purchasing, e-banking or e-communication etc)?
   (User Authentication, Server Authentication, Security from Intruders, All of the above)

8. Generally you are using password for e-purchasing, e-banking or e-communication etc, but if one more tier of security is added with the use of fingerprint for these transactions to be completely secure than what is the possibility of acceptance for the user?
   (High, Medium, Low, Not Sure)
9. Adding one more tier for enhancing security may result in some additional cost to few users, what is the possibility of acceptance that for enhancing security user can bear the nominal cost?
   (High, Medium, Low, Not Sure)
10. If any prototype could result in complete security for e-purchasing, e-banking or e-communication etc then what is the possibility of user's willingness to purchase that?
    (High, Medium, Low, Not Sure)

On the basis of replies given by the users complete analysis report is prepared and hence proved that there is need of generating an Ideal Password Authentication Scheme which would result in fortification of transport layer security protocol.

III. ANALYTICAL REPRESENTATION OF THE PARAMETERS OF THE SURVEY

On the basis of the parameters discussed in Section II, a survey was conducted to develop an idea that an Ideal Password Authentication Scheme is required which could fortify transport layer security protocol. Analysis is done on three different basis:

i. Choice of the user.
ii. Choice on the basis of Gender.
iii. Choice on the basis of Age.

I. Choice of the user: This objective states that user's choice is always the prime concern for any advancement in technologies. Security of the passwords and tokens is the most concerning challenge in the online transactions, so the choice of the user to add one more tier of security by assimilating fingerprint as the authentication parameter is required. Password along with fingerprint would be an ideal password authentication scheme which will result in the fortification of transport layer security protocol. Survey has shown that user's could bear an additional nominal cost for the prototype which would result in complete security at the transport layer for online transactions. This prototype would assimilate fingerprint along with the password for adding one more tier of security. The survey has shown following results through the bar charts, if the choice of the user is considered as one of the prime objective, for the above said parameters in Section II.

Password is the most common and accepted authentication method for online transactions which is generally used by the users.

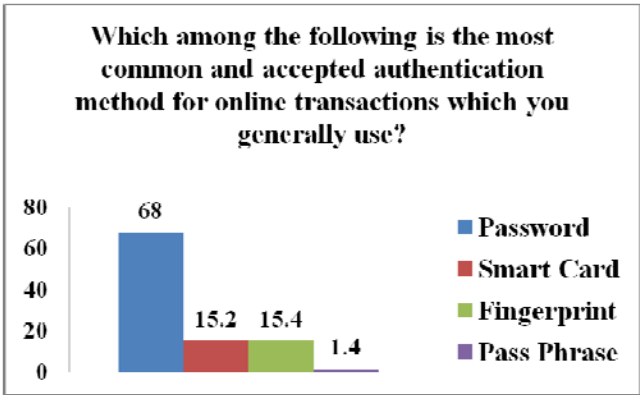

Fig: 1: Choice of authentication method for online transactions which is generally used

Security is the most concerning challenges in online transactions.

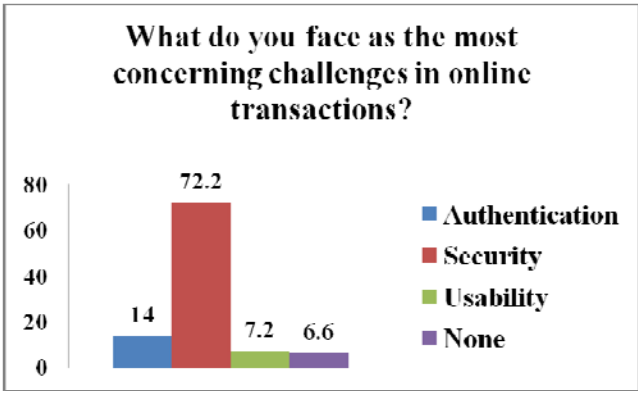

Fig: 2: Most concerning Challenge in online transactions
Passwords and Tokens have medium security during online transactions.

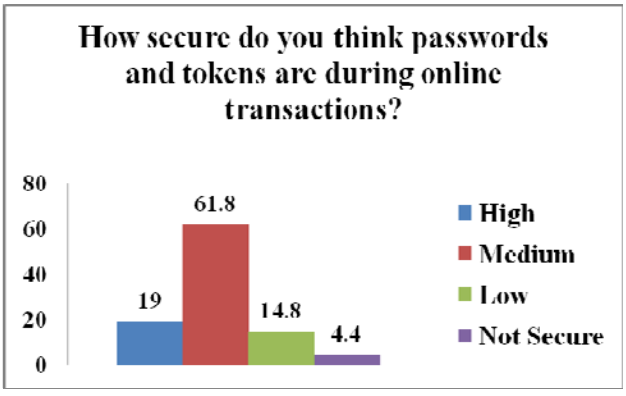

Fig: 3: Security of Passwords and Tokens during online transactions

Users perceive usability of passwords and tokens at medium level during online transactions.

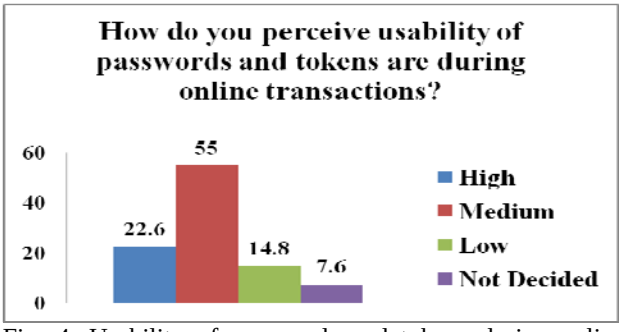

Fig: 4: Usability of passwords and tokens during online transactions

In future users would prefer fingerprint as authentication parameter for online transactions.

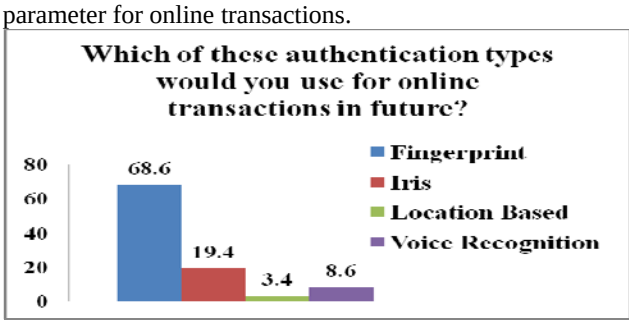

Fig: 5: Choice of authentication types for online transactions in future

Security and privacy would be at highest level if fingerprint is used as an authentication type. Fingerprint would be assimilated with the password for adding one more tier of security at the transport layer. For complete security fingerprint should be used as an authentication parameter.

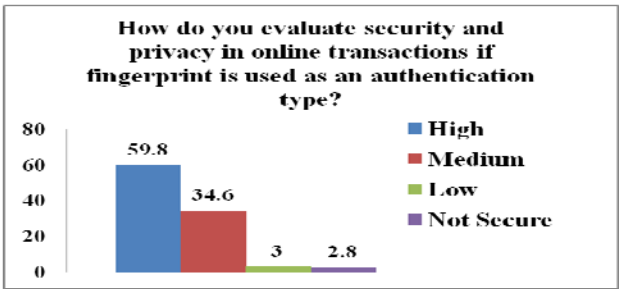

Fig: 6: Security and Privacy in online transactions if fingerprint is used as an authentication type.

User authentication, Server authentication and security from intruders are expected by majority of the users for secure transactions while using online mode either for e-purchasing, e-banking or e-communication etc. If user and server authenticate each other then mutual authentication would be done. It will result in security from intruders at the transport layer.

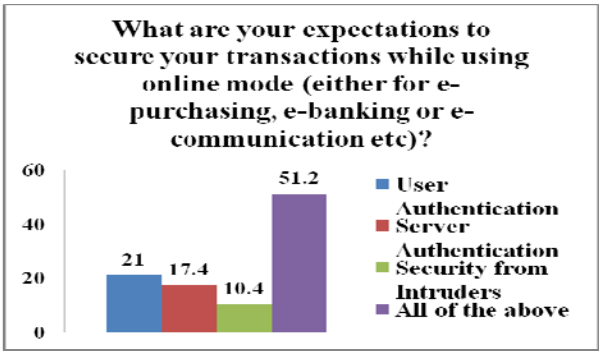

Fig: 7: Expectations to secure your transactions while using online mode

If fingerprint is used as the authentication parameter in online transactions then possibility of acceptance of data being completely secure is very high. By assimilating fingerprint with passwords would add one more tier of security in the online transactions. This assimilation would result in fortification of the transport layer.

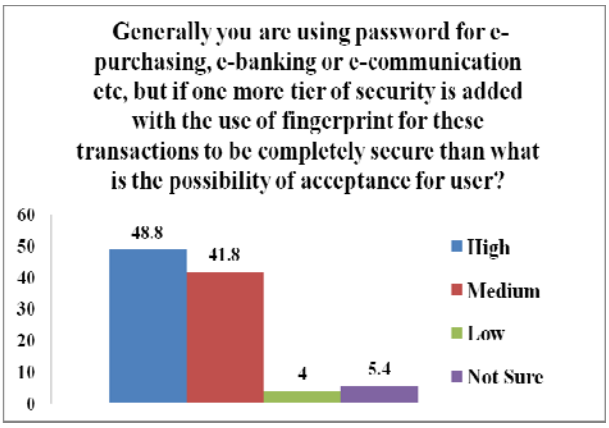

Fig: 8: Use of fingerprint makes online transactions completely secure

By adding one more tier for enhancing security may result in some additional cost, so the possibility of acceptance to bear that nominal cost for enhancement of the security is at medium level by the users.

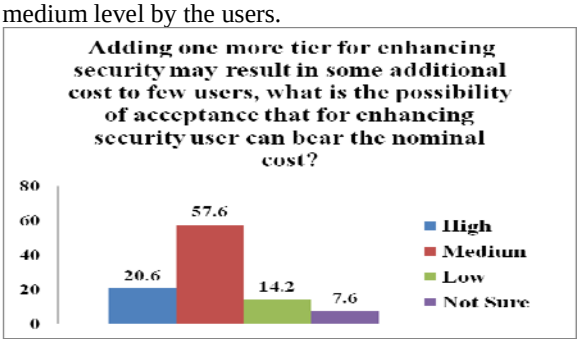

Fig: 9: Possibility of acceptance for enhancing security to bear the nominal cost

Any prototype (Assimilation of Password and Fingerprint) which results in complete security for e-purchasing, e-banking or e-communication etc then the possibility of user's willingness to purchase that is maximum. Users can bear additional cost for getting complete security in online transactions.

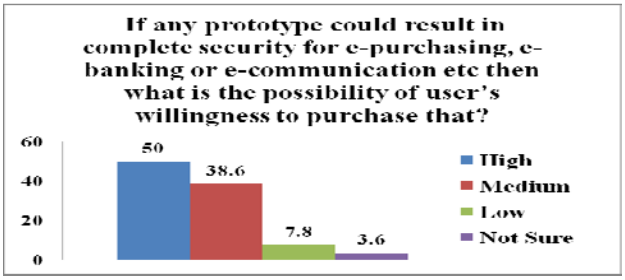

Fig: 10: Users willingness to purchase the prototype which results in complete security in online transactions.

II. Choice on the basis of Gender: During survey it is analyzed that sometimes decision varies to some percentage on the basis of gender. As far as technology is concerned male and female has different opinion. Survey has resulted that gender has major impact over an ideal password authentication scheme which will result in the fortification of the transport layer security protocol. Proof is generated through the survey that fingerprint and password together being used as authentication parameter would enhance the security at the transport layer. There is need for one more tier of security at the transport layer which would be done through fingerprint. There is high possibility of bearing extra cost for complete security. The result is shown through the following bar charts.

Parameter I of Section II: Password is generally used as authentication method during online transactions.

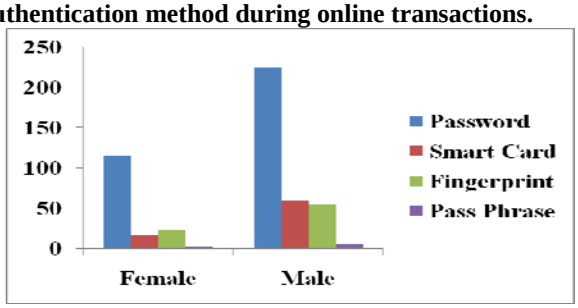

Fig: 11: Choice on the basis of Gender of authentication method for online transactions which is generally used

Parameter II of Section II: Security is the most concerning Challenge for online transactions.

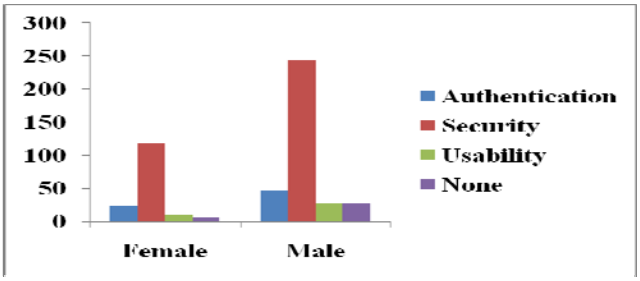

Fig: 12: Choice on the basis of Gender for most concerning Challenge in online transactions

Parameter III of Section II: Password and Tokens have medium level security in online transactions.

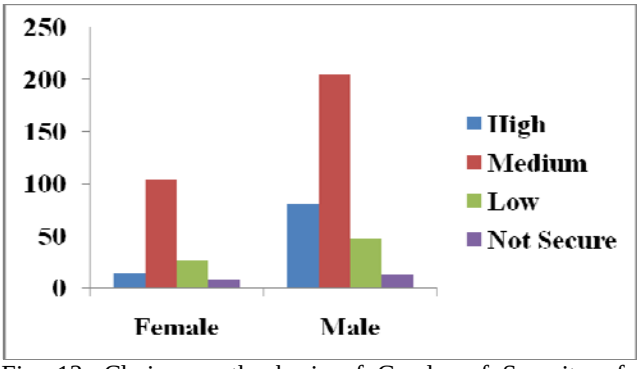

Fig: 13: Choice on the basis of Gender of Security of Passwords and Tokens during online transactions

Parameter IV of Section II: Medium usability of passwords and tokens is there, during online transactions.

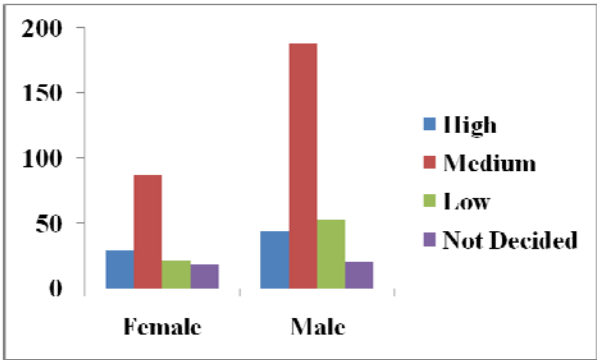

Fig: 14: Choice on the basis of Gender of Usability of passwords and tokens during online transactions

Parameter V of Section II: Fingerprint to be used as authentication type in future for online transactions.

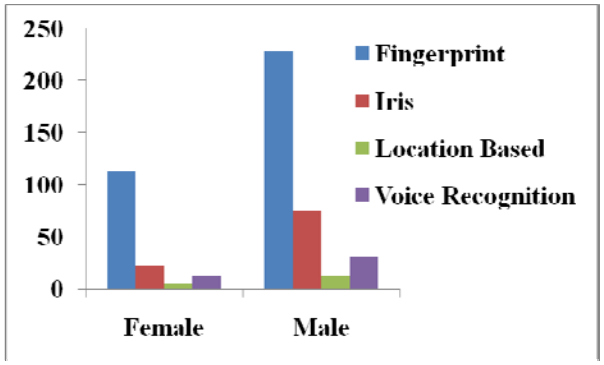

Fig: 15: Choice on the basis of Gender of authentication types for online transactions in future

Parameter VI of Section II: Security and Privacy in online transactions is high if fingerprint is used as an authentication type.

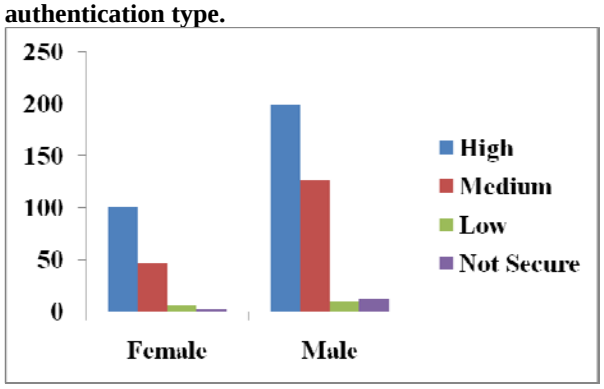

Fig: 16: Choice on the basis of Gender of Security and Privacy in online transactions if fingerprint is used as an authentication type.

Parameter VII of Section II: User Authentication, Server Authentication and Security from intruders are required in online transactions.

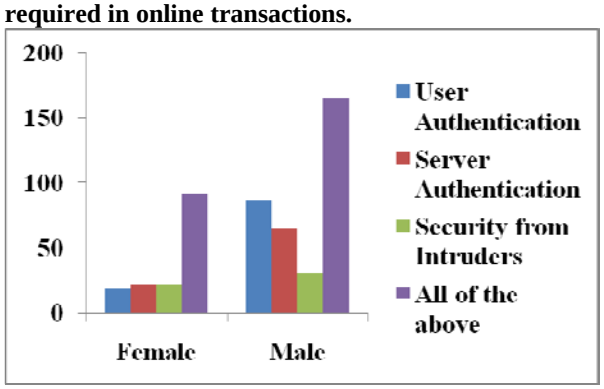

Fig: 17: Choice on the basis of Gender of Expectations to secure your transactions while using online mode

Parameter VIII of Section II: Transactions would be completely secure at the transport layer if fingerprint would be used as an authentication parameter.

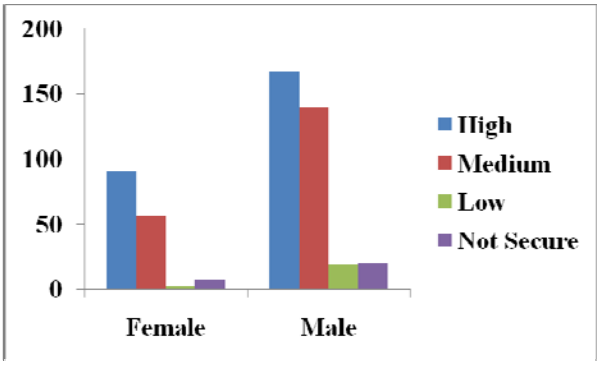

Fig: 18: Choice on the basis of Gender of Use of fingerprint makes online transactions completely secure

Parameter IX of Section II: Individual can bear nominal cost for enhancing security.

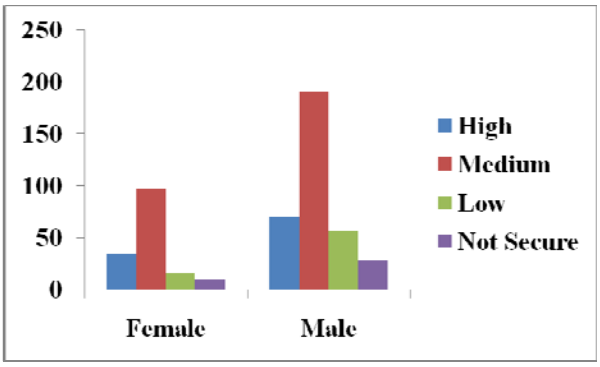

Fig: 19: Choice on the basis of Gender of Possibility of acceptance for enhancing security to bear the nominal cost

Parameter X of Section II: User's have high willingness to purchase prototype which results in complete security in online transactions at a nominal cost.

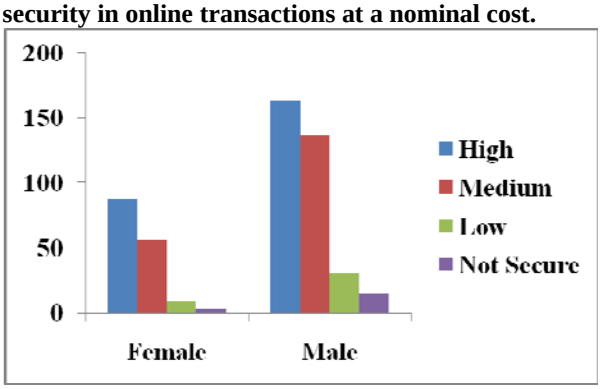

Fig: 20: Choice on the basis of Gender of Users willingness to purchase the prototype which results in complete security in online transactions.

III. Choice on the basis of Age: Decision of ideal password authentication scheme varies on the basis of Age. As the individual at the age of 17 or 25 or 35 etc, their bent towards technology would

vary. Survey has analyzed that there is need of generating an ideal password authentication scheme on the basis of age groups. This ideal password authentication scheme would result in fortification of the transport layer security protocol. This ideal password authentication scheme would assimilate fingerprint with the password for complete security at the transport layer. In the survey four age groups are defined: 17-22, 23-28, 29-34 and 35-41. The result of the survey is depicted through the following bar charts on the basis of the above mentioned age groups.

Analysis of Survey for Age group 17-22: Overall analysis of this age group is that fingerprint should be assimilated along with password for generating an ideal password authentication scheme which would result in the fortification of transport layer security protocol.

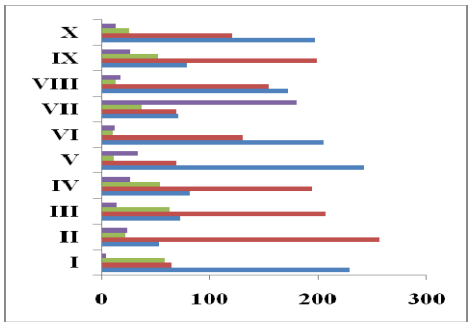

Fig: 21: Choice of Parameters on the basis of age group 17-22.

Analysis of Survey for Age group 23-28: Overall analysis of this age group is that fingerprint should be assimilated along with password for generating an ideal password authentication scheme which would result in the fortification of transport layer security protocol.

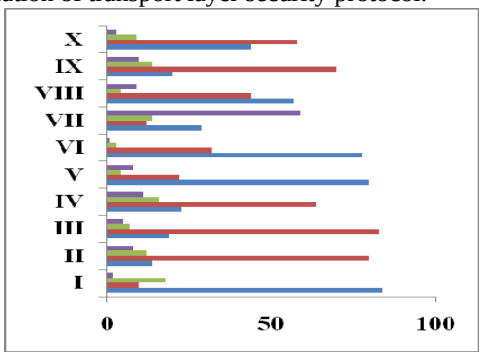

Fig: 22: Choice of Parameters on the basis of age group 23-28.

Analysis of Survey for Age group 29-34: Overall analysis of this age group is that fingerprint should be assimilated along with password for generating an ideal password authentication scheme which would result in the fortification of transport layer security protocol.

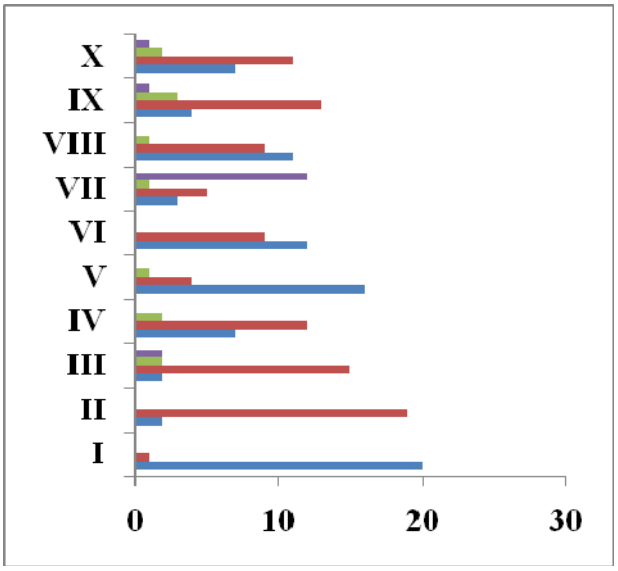

Fig: 23: Choice of Parameters on the basis of age group 29-34.

Analysis of Survey for Age group 35-41: Overall analysis of this age group is that fingerprint should be assimilated along with password for generating an ideal password authentication scheme which would result in the fortification of transport layer security protocol.

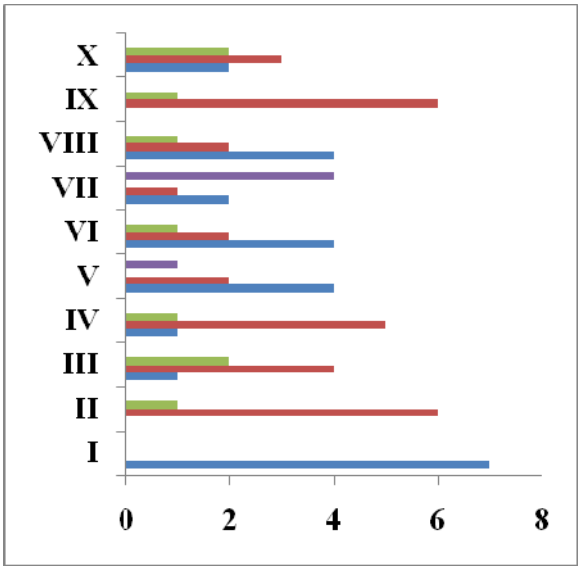

Fig: 24: Choice of Parameters on the basis of age group 35-41.

Overall analysis of all age groups is that they generally use passwords for online transactions. In future they would use fingerprint as authentication parameter. For complete security they are ready to bear additional cost over the prototype. User and Server authentication along with security from intruders is required by all the age groups.

IV. ANALYSIS OF SURVEY RESULTS

Overall analysis of the Survey on the basis of Choice of the user, on the basis of Gender and on the basis of age:

i. Password is the most common and accepted authentication method for online transactions which is generally used by the users.
ii. Security is the most concerning challenges in online transactions.
iii. Passwords and Tokens have medium security during online transactions.
iv. Users perceive usability of passwords and tokens at medium level during online transactions.
v. In future users would prefer fingerprint as authentication parameter for online transactions.
vi. Security and privacy would be at highest level if fingerprint is used as an authentication type. Fingerprint would be assimilated with the password for adding one more tier of security at the transport layer. For complete security fingerprint should be used as an authentication parameter.
vii. User authentication, Server authentication and security from intruders are expected by majority of the users for secure transactions while using online mode either for e-purchasing, e-banking or e-communication etc. If user and server authenticate each other then mutual authentication would be done. It will result in security from intruders at the transport layer.
viii. If fingerprint is used as the authentication parameter in online transactions then possibility of acceptance of data being completely secure is very high. By assimilating fingerprint with passwords would add one more tier of security in the online transactions. This assimilation would result in fortification of the transport layer.
ix. By adding one more tier for enhancing security may result in some additional cost, so the possibility of acceptance to bear that nominal cost for enhancement of the security is at medium level by the users.
x. Any prototype (Assimilation of Password and Fingerprint) which results in complete security for e-purchasing, e-banking or e-communication etc then the possibility of user's willingness to purchase that is at maximum. Users can bear additional cost for getting complete security in online transactions.

Overall analysis of Gender and all age groups is that they generally use passwords for online transactions. For complete security one more tier of security is required at the transport layer. In future they would use fingerprint as authentication parameter along with the Password. This would be an Ideal Password Authentication Scheme. For complete security users are ready to bear additional nominal cost over the prototype. This prototype would have assimilation of fingerprint along with the Password. User and Server authentication along with security from intruders is required by all the users.

V. CONCLUSION

This survey has resulted that there is need of generating an Ideal Password Authentication Scheme which will result in fortification of transport layer security protocol. Sample area of Punjab was taken which comprised of Universities, Colleges, Banks, Courts and Schools etc. Generally passwords are used by majority of the users for online transactions but for complete security one more tier of security at the transport layer is required.

Survey has stated that along with password one more authentication parameter is required. As per majority of the users in future Fingerprint should be used along with the password. Assimilation of fingerprint along with the password will be done to generate an Ideal Password Authentication Scheme. This Ideal Password Authentication Scheme will be used in all online transactions through a prototype and users are ready to pay nominal cost for purchasing this prototype. Online transactions will be extremely secure with the use of two authentication parameters. IP or Server spoofing will almost diminish. And above all this Ideal Password Authentication Scheme will result in the fortification of the transport layer security protocol.

VI. ACKNOWLEDGEMENT

We want to personally thank our students Soumik Dey, Pankaj Kumar Rai and Vakul Sharma who contributed for the smooth conduct of the survey in the various parts of Punjab. Organizations like Universities, Colleges, Banks, Courts and Schools are the part of the Survey. We thank all the individuals of these organizations who contributed for generating efficient results through a survey. Thanks to our students Maninder Singh, Anshu Anand, Ram Modi, Saurabh and Varinda Sharma who helped us for aggregation of data of the Survey. Many faculty members Mr.Jitendra Singh, Mr.Manish Nagpal, Dr.Anand, Ms.Kamini and Mr.Abhinav gave their inputs for compilation of the results.