International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

E-mail Clustering with oPass Security Prevent to Password Stealing and Password Reuse Attack

Gore Kranti K[1], Jarali Vilas M[2]

[1]PG Student, M.B.E.S .College of Engineering, Ambajogai

[2]PG Department, M.B.E.S College of Engineering, Ambajogai

Abstract: ***This paper presents a new framework for email clustering with oPass security. User mostly used text password for simplicity. Most users has multiple accounts of Gmail, yahoo and other websites they are separately login on each account and hence end up spending a more time in accessing them. It becomes a difficult task to remember all email ids and passwords for all their accounts. This paper presents a simple and single technique of which we club all the user's accounts into one account. It presents a framework for cluster or group of different email id account. The user authentication protocol (OPass) used to protect user identity. OPass only requires each participating website possesses a unique mobile number, and registration and recovery process done by telecommunication service provider (TSP).TSP phases use for the creation of one-time password. Now a days text password easily hacked and hacker access all information all other accounts of user. OPass is efficient and inexpensive compared with the other web authentication mechanisms. Therefore OTP mechanism that has implement security using private key infrastructure is used to prevent accessing sensitive information data integrity and problem due to phishing attack and key-loggers. User use SMS (short message service) for receive email notification, one time password send by the server. This system help to preventing attack mainly phishing attack, key-loggers, and password reuse attack***.

Keywords: Clustering, Email, OPass, password reuse attack, password stealing attack, phishing attack

1. Introduction

Electronic mail (Email) is used for sharing documents, files, audio and video data. There are various site provides email facility such as Google, yahoo, Rediffmail, Hotmail, etc. every system has own authentication process for logging in into their system. User uses this system according to process of email services. Every user has two or more emails, so remembering all user id and passwords it's very difficult task. If user wants search mail and recollect from all site.Then lot of time consume access each mail from all sites and also authentication process very lengthy. This paper presents clustering of email if we login at once time and access all email accounts. For more authentication provides here oPass security, when user login into the email account then OTP generates on user mobile such as short message service (SMS) therefore it provides preventing to password stealing and password reuse attack.

Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even user know the passwords is weak and it's easily predict by hacker and it's not safe.

Another critical problem is that users use similar password across various websites. Password reuse attack causes users lose sensitive information stored in different websites if a hacker attempts to obtain one of their passwords. This attack is referred to as the password reuse attack. Therefore, it is important to take human factors into consideration when designing a user authentication protocol [1].some user has different user id and different password but there difficulties for memorizing. Sometimes user thinking about same password but there chances of hacking. This paper overcomes all drawbacks using oPass security and clustering two or more Emails. OPass helps for generating OTP (one time password) on your cellphone.

This security system prevents to anti-malware, phishing attack, and password reuse attack. Telecommunication service provider (TSP) uses generating OTP and it provides two phases registration and recovery phases. TSP is way communication between user cellphone and server. In this paper two techniques are implement one is user authentication protocol named oPass and second is Email clustering. For remembering all web sites password and prevent from phishing and password reuse attack use oPass protocol. Every user have cellphone with unique mobile no when OTP generating on web server it send to user cellphone by using communication channel SMS through TSP.

There are following some attack preventing by oPass:

1) Anti-malware attack: This attack collecting sensitive information of user it include user name password credit card no etc. Keylogger is example of anti-malware attack. When user login into email clustering then oPass prevents Keylogger attack in that way hacker cannot obtain password.
2) Phishing attack: It is an E-mail fraud method .when new mail open that time some files are installed in computer and send user other sensitive information to hackers and this type of email coming from well-known site. This type of attack prevent by oPass.
3) Password reuse attack: user always choose weak password for website and also put similar password to other websites when one password leak then attacker attempt to hack other websites in that case user personal and sensitive data leaked. In oPass protocol user login when every cluster of domain that time OTP is generating on user cellphone. There is no need to remembering all passwords of different email ids. Only one time entering email clustering password and other work depend on authentication protocol oPass.

Licensed Under Creative Commons Attribution CC BY

Three factors are more important for authentication i) something you know (e.g. password) ii) something you have (e.g. smart card, token) and iii) who you are (e.g. biometric, fingerprint and other method).when user provide username and password then user authenticated by based on proven identity to granted for privileges, rights, permissions .In Email clustering user access club of email when submit OTP to the server at the time of login phase

2. Related Work

Numbers of email technique and oPass security scheme have been proposed in past some are explaining as follows:

- **Ripper learning algorithm**: In 2000 William Cohen proposed Ripper learning algorithm to identify a keyword spotting rules for classify emails. This rules based only on sender information and keyword [7]. Ripper algorithm gives only performance on keyword rule.
- **Authentication protocol:** In 2004 Wu [11]. Proposed authentication protocol which depends on only trusted proxy and user mobile device .There is need of physical account setup and it not prevent password reuse attack.
- **Phoolproof system :** In 2006 B. Parno, C. Kuo, and A. Perrig [13] proposed phoolproof system which used mobile device is used for authentication and preventing malware and phishing attack but still there is problem of password reuse attack and need of physical account setup.
- **MP-Auth protocol** : In 2007 Mannan and p.van Oorschot[12] proposed MP-Auth protocol system which uses text password and trusted mobile .There is public key installed on remote server when password sending to untrusted site it is encrypted by preinstalled public key.MP-Auth protocol help to prevent phishing and Keylogger attack but it not prevent from password reuse attack.
- **Swift file**: Information retrieval based classification by Segal and Kephart [8] used TF-IDF classifier it's also known as swift file. There are predicts three destination of incoming mail folders according to information, sometime data lost because destination of folder not fixed.
- **OPass: In** 2012 hung –min sun et.al [1] uses authentication protocol oPass for web security. User very frankly login on untrusted site, oPass system helping for reuse attack and stealing attack.
- **EmailSift:** In 2013 Manu Aery and Sharma Chakravarty [3] uses email classification method on structures and contents named as EmailSift system. In the EmailSift system uses graph mining technique to classify email into corresponding folder.

3. Background

OPass requires database, one time password, SMS channel, 3G connection.

3.1 Database

Every system need database for stored data. MySQL database used in this email clustering system .Database accepts the user details input of registration phase such as user name, password, and mobile no; no of Email ids then this database is used at the time of login and recovery phase. The credentials (ID, password) data of all users stored in encrypted form in the database. At the time of login phase the data is compared with database.

3.2 One time password

One time password (OTP) in oPass are generated by a secure one way hash function (H) .with a given input ,one time password set by hash chain through multiple hashing.one time password always use in reverse order. one time password is leaked, then attacker unable to predict the next password. One time password is produced by performing hash function on input c [1].

$$C=H\ (P_u||\ ID_S||\ Ø\ )$$

3.3 SMS channel

SMS is text based communication service. In oPass system SMS is used to resistance password reuse attack and password stealing attack. SMS represent most successful data transmission of telecom system. SMS channel have more benefits as compared to TCP/IP for security in oPass protocol. OPass prevent password stealing and reuse attack based on SMS channel.

3.4 3G connection

3G connections provide data confidentiality and data integrity to user data .3G connection useful for see incoming Email into cluster and oPass utilize the security features of 3G for registration and recovery procedure.

4. Proposed System

User always choose weak password for Email id for easily to memorization. Each User has two or many Email id and its different user id and password. This behavior causes risk of password reuse attack. Some websites generate password as random string for maintain security, even though user still change their password to simple string for easily memorization. Therefore there more chances create password stealing and password reuse attack. OPass help to resist to password stealing and reuse attack. Here two system use for remembering user id and password of all email id account and generating OTP for authentication. i) ECOPass system ii) E-mail clustering.

4.1 ECoPass System

ECoPass is Email clustering oPass system. In user authentication protocol oPass uses user cellphone for send OTP through SMS channel to user cellphone. SMS channel is secure media for communication.

Licensed Under Creative Commons Attribution CC BY

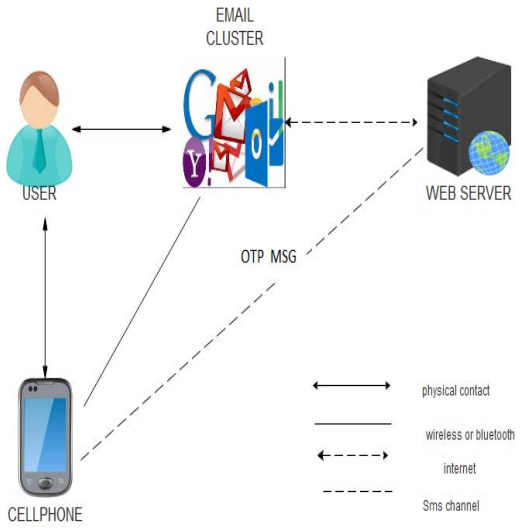

Figure 1: ECoPass system

Above figure 1 describe architecture of oPass system. User perform secure login into Email cluster for access the different Email accounts. Email cluster and web server communication done via internet. Web server send one time password to the user cellphone through SMS channel .User physically connect to the Email cluster and cellphone. User login into Email cluster then server generate OTP and send to user cellphone through SMS channel. For access Email cluster user should be enter OTP in current login session. If user enters wrong OTP then again server sends OTP to user cellphone till user entering correct OTP. If OTP message match with server database then user access the Email cluster.

The assumption in oPass system is as follows.

1) Each web server has a unique phone number. Via phone number user can interact with each website through SMS channel.
2) The user cellphone are malware Free then user can safely input the long term password into cellphone.
3) Telecommunication service provider (TSP) participated into registration and login phases. TSP is bridge between user and web server for send OTP to user. User performs registration, login, and recovery process using TSP.

4.2 Email Clustering

Clustering is technique to create a group of similar Email according to user requirements and put into different folders is called as Email clustering. In this case the main aim is to create a cluster of different Email ids account such as Google, Yahoo, Rediffmail, and other. And put into their respective folder. Email becomes an important median of communication. A user may receive twenty or hundreds of Email everyday .Handling all Email of different Email IDs account it takes much time. Therefore clustering of email provide to seen all Email of different account into cluster.
Email clustering will be carried on Email data.
1) Email data are preprocessed, following is step for preprocessing i) Removal of stop words ii) stem process.
2) Identify keywords
3) Term Frequency is calculated.
4) Similarity calculation using similarity function.
5) Clustering is done using Ecluster algorithm.

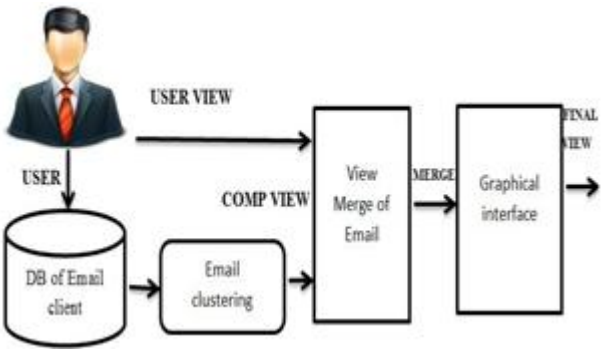

Figure 2: Email clustering.

In this framework of Email clustering the Email is cluster represented as different Email id view in single framework. Database of Email clustering is sent to, from, subject, attachment and sent-by-date etc. Make a group of all Email id accounts database in clustering. User appears in single framework all account with respective Email, therefore merge data appears to user. In Email clustering integrating all Email ids account of different site ,therefore user doesn't need of memorize all Email id accounts and respective password of Email ids account. Users only remember single user id and password of Email cluster and for their security use here oPass protocol.

5. Implementation

E-mail clustering with oPass system implementation in as follows.

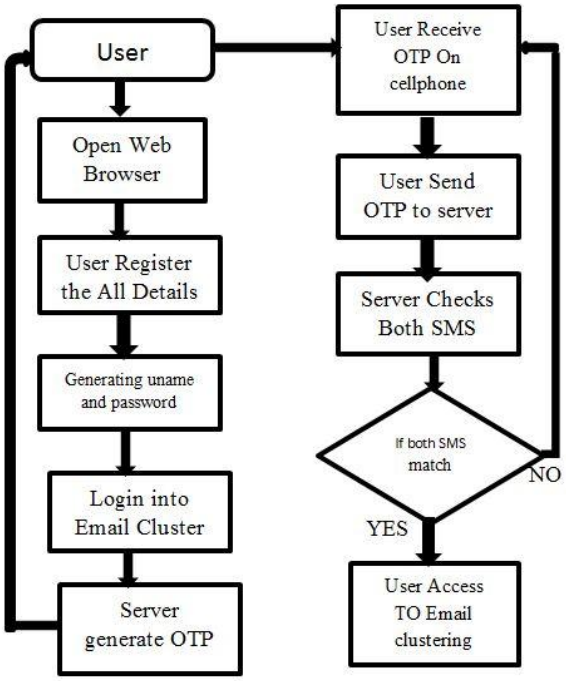

Figure 3: Operation flows of ECOPass system.

Here shows registration and login phase with oPass system. User starts with oPass protocol to register Email clustering account. Then user enters the all detail in registration form. In the registration form adding two or more Email ids account for creating cluster of Email. For authentication user must be register phone no and account id. After fill out

Licensed Under Creative Commons Attribution CC BY

registration form then generate a single user id and password of Email cluster account.

User access the Email clustering using single user id and password then open the login form and enter the user id and password that time sever send OTP message to user cellphone through SMS channel. User sends SMS to server for verification.

Server check the both data same or not. If both SMS matches then user access the email clustering if user enters wrong OTP then server again send OTP to user cellphone. This process continue user entering correct OTP.

In email clustering there is cluster of different Email id accounts such as Gmail, Rediff mail, yahoo and other. User easily access all email id account in single login procedure.

For creating a cluster of Email here uses an Ecluster algorithm. Cluster crates a group of different Email id account here using Ecluster (Email cluster) algorithm .And folder create dynamically of respective Email id accounts by using Ecluster algorithm.
Ecluster algorithm

```
BEGIN

ECluster (dataset, C)

Initialize c;       //First initialize Cluster
Old centroid=centroid
Iteration +1=1   // Cluster algo start
C'=n;    //num of cluster
Mi = {xi};    i=1……n   //min no of cluster start 1-n
do
C'=c'-1    // decrement the cluster
Find nearest cluster M    //find nearest cluster
D=dist (1, 2 (centroid 1, i) (centroid 2,j) )
Until 0=c'   //until cluster is 0
Merge MiC [maxCw];
//merge the min num cluster wait is 0//
Should stop(old centroid,centroid,iteration)
//function stop clustering//
If iteration >max _iteration;
return true
return centroid
return c cluster
END
```

Data is clustering same manner finding the data from database by using Ecluster algorithm. The main purpose of Email clustering technique is to identify clustering message in received mailbox and send to other in single framework .user can't check all email id account daily because it takes very long time. In that case easily resist password stealing and password reuse attack.

6. Result and Discussions

Performance of proposed system calculates in two ways namely ECoPass system and Email clustering. Proposed System is Email clustering with oPass system preventing password stealing and password reuse attack. ECopass system is proposed system.

Here, identify effectiveness of proposed system. Twenty two (22) people are selected and asked to work on the application each person performing registration and login phase and also measured SMS delay in registration and login phase. Following table shown performance analysis of registration and login phase.

Table 1: Result of performance analysis

System	Registration		Login	
	SMS Delay	Total	SMS Delay	Total
OPASS System	9.1	21.8	8.9	21.6
ECoPass System	8.5	20	8.1	19

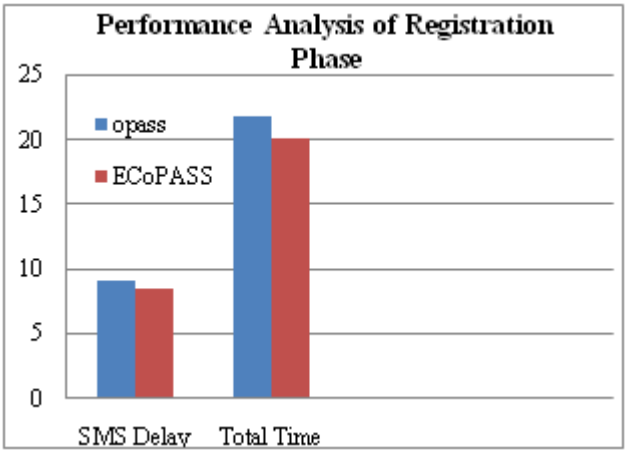

Figure 4: SMS delay and Total time of registration phase.

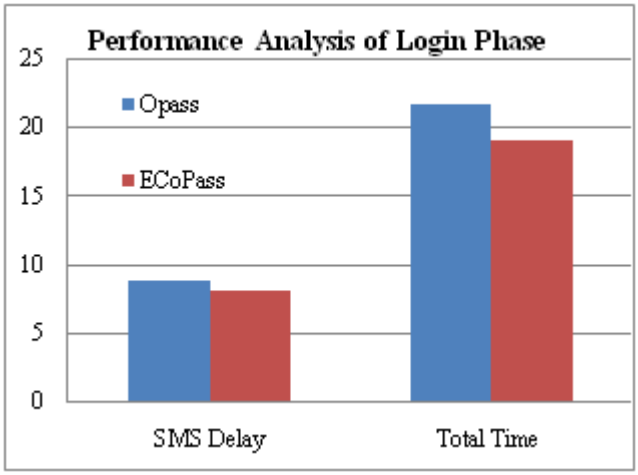

Figure 5: SMS delay And Total time of Login phase.

Here we calculated average time of SMS delay in registration and Login phase, we can observed that proposed method take less time as compared to existing system. In registration phase ECoPass system take less time. In Email clustering system when user login then access different Email id accounts at a one-time login therefore it's save time of login process. In previous system if user want to access another account data then user log out current account then login after that user access data so in that process more time take as compared to ECoPass system.

Effectiveness of email Clustering using Similarity measure for text processing is tested by implementing Ecluster algorithm. The results of Ecluster algorithm with othersimilarity measure algorithm such as Euclidian

Licensed Under Creative Commons Attribution CC BY

distance, cosine similarity. In Email clustering incoming cluster identifies and accuracy is calculated as follows:

Accuracy = (Match Counter/Length of manually created cluster +Length of System generated cluster- match counter)* 100.
Substituting value in above formula obtained a result of accuracy of different cluster.

Table 2: Accuracy of different Cluster

Accuracy OF Cluster	*Cluster 1*	*Cluster 2*
Accuracy By Cosine Similarity	36.11	20.45
Accuracy By Euclidian Dist.	24.65	25.83
Accuracy of Ecluster algorithm.	53.85	34.76

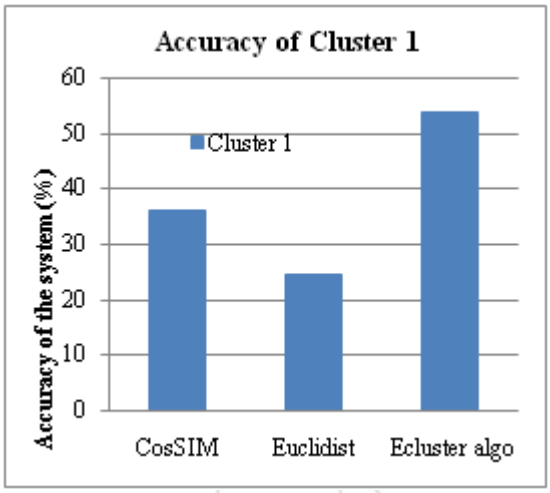

Figure 6: Accuracy for cluster 1

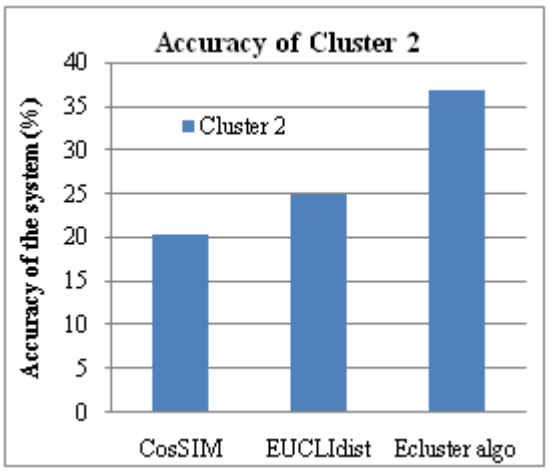

Figure 7: Accuracy for cluster 2

We observed that Ecluster algorithm accuracy is better than other algorithm. Therefore Email clustering with oPass system gives better results for clustering two or more Emails and ECoPass protocol provides more security to email users. Following table shown our system avoided attack and keep secured Email clustering. Symbol (√) shows that system avoid attack, and (○) represent not applicable. Compare proposed system with previous research.

SYSTEM	Attack Prevention						
	Session Hijacking	*Phishing*	*Key-Logging*	*Password Reuse*	*Malware Prevention*	*Password Stealing*	*DNS Spoofing*
Prop. System	√	√	√	√	√	√	√
OPass[1]	√	√	√	√	√	√	√
MP-Auth[12]	√	√	√	○	√		√
Phoolproof[13]	√	√	√		√		
Session Magnifier[14]	√						√
Secure Web[11]	√	√	√	√	√		√

Proposed system prevents mainly password stealing attack and password reuse attack as compared to others. Email clustering use logical account setup, trusted proxy, so it prevents above attack.

7. Conclusion

In this paper proposes a novel architecture for easily access Email clustering account which includes different email id accounts of user and provide user authentication protocol (oPass) avoiding all possible attack and threats. In email clustering create cluster of two more email id .when user login in cluster then OTP generate and it appear on user cellphone we know every user has unique mobile number in that way this telecommunication system also provides registration and recovery phase. OTP and telecommunication service provider (TSP) along with web services this method of authentication safe, reliable and provide data confidentiality. In this system proposed Email clustering with oPass security preventing to password reuse attack and stealing attack, when new user do registration that time all data related to email id saved into the database and when user goes to logging phase that time OTP generate for authentication and it send on users mobile then user access all email id of different domain with single password. And without OTP no one access the Email clustering data, so it helps to prevent password stealing and password reuse attack. Email classification system helps for email classify according to priorities and corresponding folder. By using ECoPass security user no need to remember long term password. Users are easily login in this framework and access email cluster.

References

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks" in IEEE transaction information forensics and security, vol no.2, April 2012 651.

Licensed Under Creative Commons Attribution CC BY

[2] Sharma C, Arvind Venkatachalam, Aditya Telang, "A Graph-Based Approach for Multi-Folder Email Classification" in 2010 IEEE International Conference on Data Mining.
[3] Manu Aery and Sharma Chakravarthy, "eMailSift: Email Classification Based on Structure and Content" in IEEE transaction information" in vol.59 no.6 April 2013.
[4] SyedaFarhaShazmeen, JayadevGyani,"A Novel Approach for Clustering E-mail Users Using Pattern Matching" in 978-1-4244-8679-3/11/$26.00 ©2011 IEEE.
[5] Ms. Karthiga, K. Aravindan, "Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks" in International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 8.
[6] Qinbao Song, Jingjie Ni and Guangtao Wang, "A Fast Clustering-Based Feature Subset Selection Algorithm for High Dimensional Data" in IEEE transaction on knowledge and data mining vol. 25 year.
[7] W. W. Cohen, "Learning rules that classify e-mail" in Proceedings of AAAI-1996 Spring Symposium on Machine Learning in Information Access pages 124–143, 1996.
[8] R.B.Segal and J.O.Kephart, "Swift file: An intelligent assistant for organizing e-mail" in Proceedings of AAAI 2000 Spring Symposium on Adaptive User Interfaces pages. 107– 112, 2000.
[9] J. D. Marnie, "ifile: an application of machine learning to e-mail filtering." in Proceedings of KDD-2000 Text Mining Work-shop, Boston Aug, 2000
[10] S. Kiritchenko, S. Matwin, and S. Abu-Hakima, "Email classification with temporal features " in Intelligent Information Systems, 2004 pp. 523–533.
[11] M.Wu, S. Garfunkel, and R. Miller, "Secure web authentication with mobile phones." in DIMACS Workshop Usable Privacy Security SoftwareCiteseer, 2004.
[12] M. Mannan and P. van Oorschot, "Using a personal device to strengthen password authentication from an untrusted computer" in Financial Cryptography Data Security, pp. 88–103, 2007.
[13] B. parno,ckuo and A. Perring, "Phoolproof phishing prevention" in financial Cryptography Data Security pp. 1–19, 2006.
[14] C. Yue and H. Wang, "Session Magnifier: A simple approach to secure and convenient kiosk browsing " in Proc. ACM 11th Int. Conf. Ubiquitous Computing, 2009, pp. 125–134

Author Profile

Gore Kranti K received BE degree in computer science and Engineering in 2014 from Dr.babasaheb ambedakar marathwada university, Aurangabad. She is currently PG student of Computer networking and Engineering department in M.B.E.S.C.O.E Ambajogai .Her research include network security, cryptography and information security.

Jarali Vilas M received the M.Tech degree in computer science and Engineering in 2011. And BE degree in 2009 from Veshveshwaraya Technological University (VTU), Belgaum India. He is currently assistant professor in PG department in M.B.E.S.C.O.E Ambajogai from 2013 to till date. His research interest includes network security, 4G network and communication network.

Licensed Under Creative Commons Attribution CC BY