Simplex Email: Controlled Access of an Email Account among the Users of a Cluster

Shirisha Kakarla
Dept of CSE,
Sreenidhi Inst.of Sc. & Tech.,
Hyderabad – 501301, India

Archana Nagelli
Dept of CSE,
Sreenidhi Inst.of Sc. & Tech.,
Hyderabad – 501301, India

Geeta Vemula
Dept of CSE,
Sreenidhi Inst.of Sc. & Tech.,
Hyderabad – 501301, India

ABSTRACT
In this paper, we have addressed a scenario, where a group of people are in need to access the common files of enormous size through mails. However, the space constraint observed in the mailbox of an individual, be in the public domain or in the private domain, either due to insufficient remaining space or the allocated space, the considerably large files cannot be communicated. We have proposed a simplex mail account, meant for people within an organization, academic institution, government, etc., wherein the bigger files can easily be stored and accessed through mail. The simplex mail account is a single mail account and can be viewed by number of people with two sets of privileges. Though a single mailbox is accessed with number of people simultaneously, the security issues are as good as the ones being offered by the other mailing systems already available.

Keywords
simplex mail account, authorization, two-factor authentication, repudiation, denial of service.

1. INTRODUCTION
Now-a-days, the most pervasive mode of communication among the users accessing the internet is the email messaging system. Number of websites and hosts offer the email services and mostly they are free of charge to the subscribers. The subscribers to these public email services can access the services, like sending/receiving emails and/or files of different formats, permitted by their respective hosts. Though the storage space allocated by the hosting website to each subscriber of mailbox is specific and limited, virtually no restriction on the storage space is encountered by the majority of the users. However, the same amount of storage space is considered to be insufficient by the few email users, who are in need to transfer bulky content in their emails. Thus, files and/or data of enormous size are rather be stored in the other storage media like compact disks, flash drives, etc. and transferred physically. The email messaging services cater to the issues related to the transfer of personal communication.

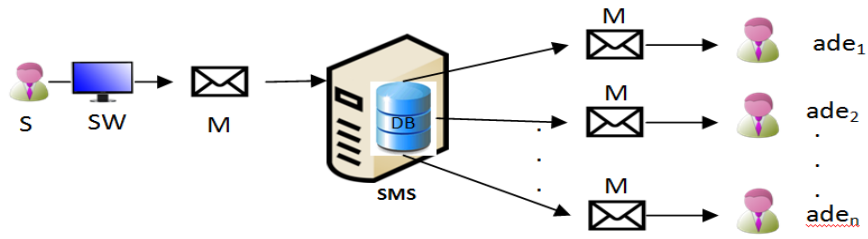
The same mailbox is considered to be unethical for use in transferring messages or information related to the profession/business. Consider a case, where a person, subscribed to a public email service, is an employee working in the office of Auditor General. The employee is responsible to oversee the accounts and audit the quarterly reports periodically, in the office. The information so processed should be protected from the malicious use by the outsiders. However this information pertaining to the auditing process needs to be shared among the authorized employees and the employer, within the same organization. For this purpose, using the public mailbox is eventually threatening and is always vulnerable [1][2][3]. In order to secure this communication, most of the organizations have their own email messaging services registered with their domain. This gives an opportunity to the employer and the employee to send and/or receive emails pertaining to the information of their profession.

In general, most of the organizations are opting for Remote Desktop Connection [4][5] logging systems, either open source or proprietary, for sharing large files among the employees. However, this mechanism too suffers from two issues, discussed a little later.

In this paper, we are putting forward a novel concept in the mailing system, the simplex email account. The term simplex is derived from the study of Communications wherein, the term simplex refers to one-way communication between two parties. The similar communication exists in our mail account too. This is best applicable to the case, where big data files are to be shared among the authorized people across the globe through mail account. The users of this mail account can only view the content and cannot manipulate the data or account settings, whatsoever, apart from the privileged one. In order to create this mail account, out of the total storage space allocated for mailing system, within an organization, considerably bigger part is allocated to this new mail and the remaining is partitioned as smaller chunks for each individual mailbox.

The plan of the paper is as follows. Section 2 discusses briefly about the existing mailing systems. The Section 3 describes simplex email account creation, access privileges and management. The sub-section 3.1 suggests the pseudo-code and the illustrative snapshots of the UI part of the simplex mail account creation and user enrollment. In the Section 4, the conclusions are drawn and the future work directions are mentioned.

2. EXISTING SYSTEM
In the existing system, one way of communicating electronically, between an employer and employees, is a group mail created within their private domain, as shown in Fig.2.1 (a). For example, auditdept@sreenidhi.edu.in is the group mail account of the employees associated with the audit department of an educational organization, namely, Sreenidhi. Alternatively said, the professional email account of each employee working in the audit department of Sreenidhi is enrolled in a group: auditdept. An email being sent to this group mail account is received in the mailbox of each individual of this group. Thus, all the members of the group will have the copy of the same email.



S : Sender
SW: Sender Workstation
M: email message to auditdept@sreenidhi.edu.in
SMS: Sreenidhi Mail Server
DB: SMS database embedding n independent partitions for n individual users of the group mail account: auditdept@sreenidhi.edu.in
$ade_{1, 2, ...n}$: **a**udit**d**ept **e**mployee 1.2….,n of sreenidhi grouped in the auditdept group mail account

Figure 2.1. (a) Group Mail Account Scenario

Despite the fact that, many organizations, in the recent past, are able to afford to have their own domain and the related email services in place; the storage space is still one of the major bottlenecks. As each employee, in such case, has his own professional mailbox registered with the domain, his mailbox is allocated with a specific amount of storage space in the overall storage space available, as shown in the DB component in Fig. 2.1 (a). All the partitions put together make the actual storage space. The size of the storage partition restricts the employee in sending or receiving the content/files of excess size through emails.

One way of overcoming the restriction of limited storage space is to provide a common email-id, which can be accessed by all the employees of a group, as depicted in Fig. 2.1(b).

Accessibility of this email account is done through the password that is conveyed to all the employees, secretly. Unlike in the group mailing system where the available storage space is divided into number of partitions, here, substantially bigger space block can be allocated to the common email account. The sender to this email account can send the large amount of data, virtually.

This is advantageous in case where the employees need to access the common data of large size. Few examples of the large sized data are employee rule book, yearly audit reports, installation files, etc.

The weakness of using a common email account is manifold. As the access rights of the users over the common mailbox are not restricted, the users may accidentally or intentionally mishandle the data present in the mailbox. The data misuse may involve message/file deletion leading to repudiation [6][7] of communication, upload irrelevant information, redirecting the mail to their personal mails. Apart from these, misuse of the access rights may lead to denial of service (DoS), because of password change by either of the users. Users may change the settings of the account like disabling the 'save in the sent mail' option, deleting the contact(s) in the address book, renaming the entries in the address book, disabling the signature, changing the default primary account, and so on. However, the threats [8][9] posed by the disgruntled employee from the intentional misuse of the allocated privileges are far more serious than the accidental misuse.

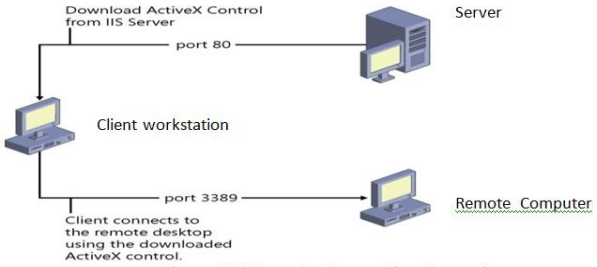
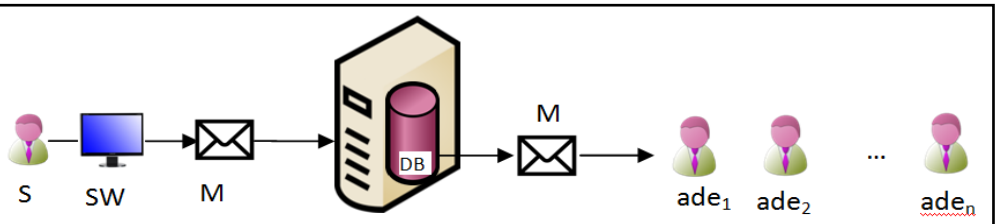


Figure 2.2 Remote Connection Scenario

The remote connection, as shown in Fig.2.2, another widely used mechanism [4][10] to share the large data, speaks about two issues. The accessing of data among the employees within an organization is primarily possible when they are sharing a common network.

Secondly, the node in which the data is stored have to be enabled with remote connection privilege, so that the other



S : Sender
SW: Sender Workstation
M: email message to auditdept@sreenidhi.edu.in
SMS: Sreenidhi Mail Server
DB: SMS database with a single partition accessed by n users with same privileges
$ade_{1, 2, ...n}$: **a**udit**d**ept **e**mployee 1.2….,n of sreenidhi grouped in the auditdept group mail account

Figure2.1 (b) Common Mail Account Scenario

nodes of the same network can identify and access the data available. Unlike in the group mailing system, restriction on the size of data to be accessed is largely overcome in remote connection mechanism. However, the benefits of the email, either group or single mailbox accessed by many even in the public networks, is restricted in remote connection mechanism because of the second issue. Though open source means are there in the market which can offer the remote connection accessibility by creating virtual private network within a public network economically; they are limited in access time and amount of the data to be transferred. Few proprietary softwares are able to address these drawbacks with a cost.

3. SIMPLEX EMAIL ACCOUNT AND ACCESS PRIVILEGES

We, in this section, describe the creation of an email service, namely simplex email for sharing data of large size among the users of a cluster. A cluster is identified, manually, as a group of people with similar requirements. For example, students of a class, employees of a section in an organization, members of a training course group, and so on. In contrast to the group mailing system, simplex email is a singular mail account, i.e., a single set of username and password, and is accessed by multiple users with the same username and password. The diagrammatic representation of the simplex email is shown in the Fig. 3.1.

The simplex email, though, can be accessed by the multiple users; the privileges assigned to the users are varying. This can be explained in the following manner. The total number of users within a cluster is divided into two groups. One group is comprised of merely a single administrator, namely Admin. The second group involves the remaining users of the same cluster.

The roles and responsibilities of an administrator can be defined as follows:

He registers to the simplex email with appropriate username and password.

He then selects a security question of his choice with his own relevant passphrase. This acts as a profile security measure. The completion of registration process lead to the triggering of two tasks:

Task a) A new table (say UsersDB_auditcluster in our case), with the schema and description mentioned below in Fig. 3.2, is generated in the UsersDB database for this simplex email account, to accommodate the details of the Admin and the proposed users for this particular simplex account.

Task b) A unique web-link is generated and embedded in an automated message along with username, password, security question, security answer and sent to the personal email account mentioned during the registration process to the Admin.

EmpID: unique employee ID assigned to the employee in the organization

Profile Name: Role of a permitted employee for the simplex mail account from the domain {Admin, User}.

EmpName: Name of the Employee

Personal Email Account: Email-id of an employee belonging to a cluster in an organization and is expressed in the symbolic representation as shown in the Illustrative UsersDB_auditcluster table.

Mobile Number: 10-digit unique contact number

Confirmation: It indicates the status of the information received by the user about the username and password of the simplex email account. The domain of this attribute is {yes, no}. By default it is marked as 'no', i.e., the user is yet not informed or confirmed the knowledge about the account username and password. Thereafter, when the user clicks the web-link in the message from his personal email account, it changes to 'yes'.

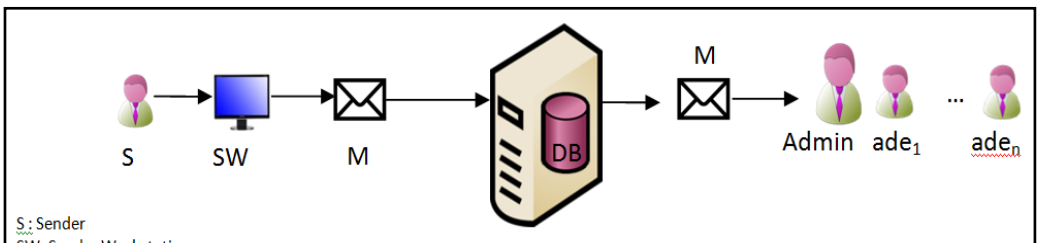
Figure 3.2 Schema for a new table in UsersDB Database

The administrator views the message and confirms the registration by clicking the web-link.

The administrator is also responsible for enrolling the users of the second group by giving credentials of each of them like employee identification (EmpId), employee name, employee's personal email account and the respective mobile phone number. The illustrative entries showing the details of the users of the second group can be seen in the Table 1 given below.

Others can communicate to this email account for conveying content that can be accessed by all the users as well as the Admin of this simplex account in a way as good as they communicate with the group mail account, albeit with an advantage of increased storage space.

Similarly, upon successfully enrolling, the administrator can access this email account for sending a message or uploading the content intended for all the users to this simplex mail account. These privileges he can execute by providing the answer to the security question that he had chosen for his



S : Sender
SW: Sender Workstation
M: email message to auditdept@sreenidhi.edu.in
SMS: Sreenidhi Mail Server
DB: SMS database with a single partition accessed.
Admin: administrator
$ade_{1,2,...,n}$: auditdept employees 1.2....,n of sreenidhi grouped in the auditdept group mail account

Figure 3.1 Simplex Email Account Scenario

profile. This acts as a two-factor authentication process.

He also can modify the simplex mail account password, in case the current password is compromised.

Table 1. An Illustrative UsersDB_auditcluster Table

EmpID	Profile Name	Emp Name	Personal Email Account	Mobile Number	Confirmation
1208	Admin	Shirisha K	shirishak@sreenidhi.edu.in	9783517384	no/yes
1209	User	Archana Nagelli	archananagelli@sreenidhi.edu.in	9783517587	no/yes
1350	User	…	^([0-9a-zA-Z])([0-9a-zA-Z])*@sreenidhi.edu.in$	\d{10}	no/yes
…	User	…	^([0-9a-zA-Z])([0-9a-zA-Z])*@sreenidhi.edu.in$	\d{10}	no/yes
…	User	…	^([0-9a-zA-Z])([0-9a-zA-Z])*@sreenidhi.edu.in$	\d{10}	no/yes
…	User	…	^([0-9a-zA-Z])([0-9a-zA-Z])*@sreenidhi.edu.in$	\d{10}	no/yes

The old password can be disabled and a new password by using the two-factor authentication process. Meanwhile, for all the users enrolled for this particular simplex account in the UsersDB, the value under the Confirmation attribute is reset to default 'no'. Thereafter, in order to inform the users of the second group of users, the renewed password and a web-link to the registered email id of the users.

The administrator may delete the content upon request, by answering the profile security question. Likewise, he may reply and forward the mails as well.

This way, the administrator is the sole person managing the account's content and the viewers in a secure and authorized way, effectively.

The users of the second group of a particular cluster, on the other hand, can perform the following tasks:

Upon enrollment by the Admin, the intended users of the cluster receive an automated message in their registered personal mail account, as mentioned during the enrollment process, having simplex account details and a web-link in the beginning, and thereafter a new password and a web-link, in case the earlier password is renewed.

Each user can open the message and click on the web-link so provided. This, in turn, is considered as an acknowledgement sent from the user and the same is reflected under the Confirmation attribute of a unique record (pertaining to the user) by changing the default 'no' to 'yes' in the table of the UsersDB database. This confirms the receipt of the account details by the user. From this time onwards, the user of the cluster is able to access the content of the simplex email with the same username and the password.

The user can access the account by giving the same username and password, what the administrator has validated, and view the contents of it.

Like an administrator, the user also can download and/or redirect the content provided in the account, for later use.

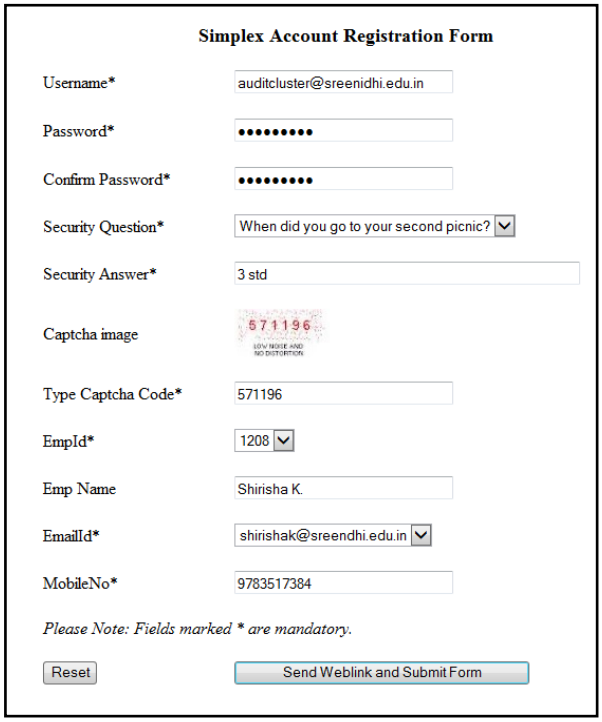
The user cannot delete any content, whatsoever, from the account. In case, the user attempts to delete, he is prompted to select the appropriate security question, which has been chosen initially, and provide the correct answer. This security measure is adopted to thwart the deletions by unauthorized users of the same cluster. As the administrator of the simplex email account knows correct combination of security question and its answer, as he has preferred it earlier, he is the only authorized one to perform any manipulations of this simplex email account.

The tasks so defined for the users are meant for passive accessing of the content from the simplex mail account.

3.1 Pseudo-Code For New Simplex Email Account Creation And The Representational Snapshots

The following is the step-wise procedure for generating a new simplex email account for a cluster of people (with one person acting as Admin and assigned with additional privileges, and the remaining as normal users with fewer privileges as that of Admin) accessing the common data within an organization.

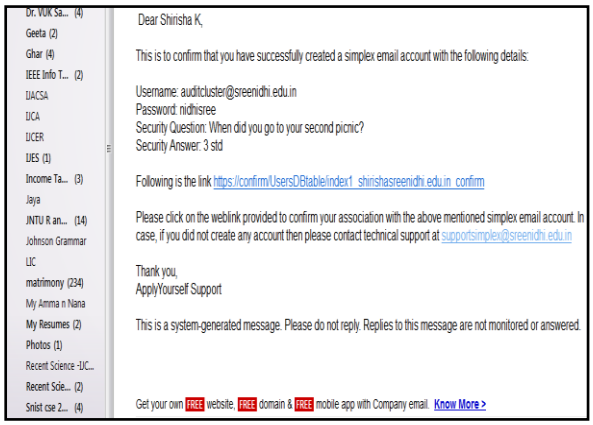
Step 1: New simplex email account creation: The Admin do the registration process for creating a new simplex email account giving the username, password, security question and security answer appropriately. He also enters the other inputs and submits the form. The representation form in shown in Snapshot 3.1 (a). As an acknowledgment, the web-link along with username and password is sent to the Admin's personal email account mentioned in the registration form.



Snapshot 3.1 (a): Registration page for creating a new Simplex Email Account

Step 2: Database Design: As a by-step of the new account creation process, a new table, namely UsersDB_auditcluster in our case, is generated in the UsersDB database, as per the schema mentioned in the Fig. 3.2. This table is populated with the details of the Admin and the users of the cluster under consideration, subsequently upon their enrollment.

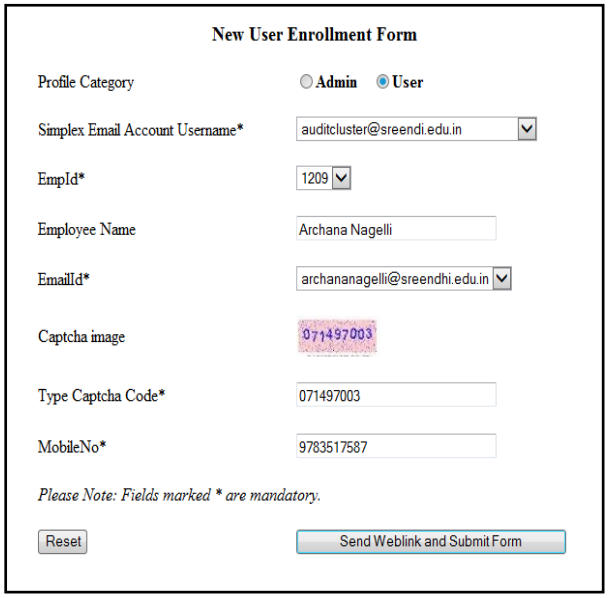
Step 3: Acknowledgement Management: The Admin, upon receipt of the acknowledgement, as shown in the Snapshot 3.1 (b), confirms his association with the simplex email account



Snapshot 3.1 (b): An Illustrative Simplex Email Account Creation Acknowledgement to the Admin

by clicking on the web-link. The same is reflected in the corresponding record of the above said table in the UsersDB database.

Step 4: New User Enrollment: The Admin, then, enrolls each individual user for accessing simplex email account, after answering the security question. The illustrative enrollment process is shown in the Snapshot 3.1 (c).



Snapshot 3.1 (c): New User Enrollment form for existing Simplex Email Account

In turn, each user receives the web-link as an acknowledgement with the account details as well. The user performs the similar action as Admin to confirm his association with the account.

The safe and unrestricted one-way transfer of the files there upon can happen to this simplex mail account from the others as well as the Admin of this account. Thus, this enhances the optimality of the limited storage space and also restricts the users from performing unprivileged actions over the data that is shared.

4. CONCLUSIONS AND FUTURE SCOPE

In the startup organizations, where storage media is one of the critical issues, the simplex email account serves an advantage for propagating common content which can be accessed by a group of people. Out of the total storage area available for a section (or a department or a cluster) in a Mail server, a bigger chunk is utilized for simplex mail account, communicating common content, and the remaining may be partitioned into smaller ones for each individual person of the same section. Thus, the data of enormous size can also be easily and elegantly stored in the simplex account. As the simplex account is singular, i.e., only one account which is accessed by more than one person, the username and password can voluntarily be shared. In the near future, we are aspiring to improve upon the features of our mail account by tracking the user details. This will put a check on the propagation of unsolicited and confidential content and its further misuse.

5. ACKNOWLEDGMENTS

We whole-heartedly thank the management of our Institute: SreeNidhi Institute of Science & Technology, Hyderabad for their financial assistance and appraisal.

6. REFERENCES

[1] Stine, Kevin; Scholl, Matthew. "E-mail Security: An Overview of Threats and Safeguards." Journal of AHIMA 81, no.4, April 2010, pp. 28-30.

[2] Schneier, B. “Secrets and Lies: Digital security in a Networked World”, New York, Wiley, 2000.

[3] National Research Council, “Computers at Risk: Safe Computing in the Information Age”, Washington, D.C: National academy Press, 1991NRC91.

[4] Cai Longzheng, Yu Shengsheng, Zhou Jing-li, "Research and Implementation of Remote Desktop Protocol Service Over SSL VPN", SCC, 2004, Proceedings. 2004 IEEE International Conference on Services Computing, Proceedings, 2004, pp. 502-505, doi:10.1109/SCC.2004.1358052

[5] Charlie Russell, Craig Zacker , “Introducing Windows Server 2008 R2”, published by Microsoft Press, 2010 , pp. 47-58.

[6] Santiago, J., Vigneron, L., “Study for Automatically Analyzing Non-repudiation”, ACI Sécurité SATIN and the IST-2001-39252 AVISPA project.

[7] Robinson, P., Cook, N., Shrivastava, S., “Implementing Fair Non-repudiable Interactions with Web Services”, Proceedings of the 2005 Ninth IEEE International EDOC Enterprise Computing Conference, EDOC 2005, 2005, 0-7695-2441-9/05.

[8] Kemp, M., “Barbarians inside the gates: Addressing internal security threats”, Network Security, 2005 (6), pp. 11-13.

[9] Hayden, M. “The Insider Threat to U.S. Government Information Systems”, National Security Telecommunications and Information Systems Security Committee, 1999.

[10] Bloomsburg University of Pennsylvania. (n.d.). Remote Desktop Connection? Retrieved from https://www.bloomu.edu/technology/remote