Public Alert System over Cellular Networks

Mr. S. P.Santhoshkumar#[1], Mr. D. Prabakar#[2], Dr. S. Karthik#[3]

[1#] *Assistant Professor, Dept of CSE, SNS College of Technology-India*
E-Mail ID: spsanthoshkumar16@gmail.com
[2#] *Assistant Professor, Dept of CSE, SNS College of Technology-India*
E-Mail ID: prabakaralam@gmail.com
[3#] *Professor & Dean, Dept of CSE, SNS College of Technology-India.*
E-Mail ID: profskarthik@gmail.com

Abstract— **In case of emergencies, the mobile text messaging services are progressively being allocated to circulate analytical information. Consequently, the third party providers promise to advance physical security by delivering such messages promptly to a wide range of organizations like colleges and universities. The main objective of this paper is to enforce security to the users during the information exchange. The text messaging allows transmitting short, alpha numeric communication for a wide variety of applications. Public Alert System (PAS) presents two components mainly Administration Management and User Management. In PAS, there is a domain connected to intranet through which the user accounts can be created. Sending of mails to other user accounts by the authorized user is allowed and inbox can be managed. The system helps the users to view, store and delete the mails when necessary. Also when the account is hacked, the hacker list along with the date, time of attack and the IP address is being stored in the user account. The user can view the hacker details by logging into appropriate account. In so doing, the system demonstrates that this infrastructure provides better security to the users since there is no hacking of mails.**

Keywords—**DNS, public alert, SMS, security**

I. INTRODUCTION

The term Mobile Computing refers to the human–computer interaction in which a computer is expected to be transported during normal usage. Mobile computing includes mobile communication, mobile hardware and mobile software. Mobile hardware includes device components or the mobile devices. Mobile software deals with the characteristics and requirements of mobile applications. The communication issues include the ad-hoc and infrastructure networks as well as communication properties and protocols[1][5]. Mobility refers to the person moving between different geographical locations, networks, applications and communication devices. Also it refers to the device that moves between different networks and geographical locations. The advantage of mobile computing is mobility and it reduces the time to order for any products. Various things can be done through mobile networks such as internet, short messaging service, etc.

Computer Networks is a collection of hardware and computers in which they are interconnected by the channels of communication. It allows sharing of information and resources between different computers in the network.

Nearly in every industrial settings and factories, the vital information between machinery, control, and monitoring devices is carried by the communication links. Much of the control and status information are transferred in the industrial settings, temperature or the liquid levels. Large file transmission can also be done in the computer networks with greater efficiency.

The third party alert system provides an efficient message delivery system during the problem of emergencies by using text messaging services. This form of communication service is offered by the cellular networks. The third party alert system is used to send the bulk messages when there is a case of emergency like tsunami, earthquake, etc. This system provides security only in the case of smaller population and it is supposed to deliver the alert messages within ten minutes of the alert goal [7]. If the messages are not delivered within ten minutes, then it is retransmitted once every 15 minutes. Some of the problems in this system are,

- It does not meet the ten minutes alert goal
- It is suitable only for smaller population
- Congestion occurs when the messages are not delivered
- No authentication is provided for the text messages.

The Public Alert System (PAS) is used to send alert messages to the users in an organization. It can also be used to send useful information to the users. This Public Alert System (PAS) provides better security to the users. Hacker List is used in the Public Alert System so that if any account is being hacked, an alert mail regarding hacking is saved in it. Similarly, an alert message is sent to the user’s mobile number thereby providing the users, a greater security [2]. The two major components in Public Alert System are Administration Management and User Management. End User has manifested by administrators with the ability to identify and control the state of users logged into the server.

The PAS consists of a domain connected to intranet. This domain helps in creating accounts for the organisation and users. Mails can be sent to any user within the registered companies and the inbox can be managed.

This infrastructure provides better security to the users since there is no hacking of mails. Also it does not achieve the advertised requirements for larger population. Administrator owns the overall determination of controls, setting of major objectives, and the identification of general purposes, guidance, leadership and control of the efforts of the groups towards some common goals. Admin also have the rights to restricts the users and give the access justices to the user to register their details.

User Module states that person should register their entropy, contact details, and login information. The users can function according to the access permission given by the administrator. User Management is a substantiation feature that provides administrators with the ability to identify and control the state of users logged in [8].

The communication across the world is important in the modern age. Communications through postal may take more time. It may take days or even weeks to make the message available to others. The electronic way of communication is managed by the E-Mail services. Deduction of spam mails includes the process of storing the malevolent program mails in the spam. Deletion of unwanted mails can be made to manage memory.

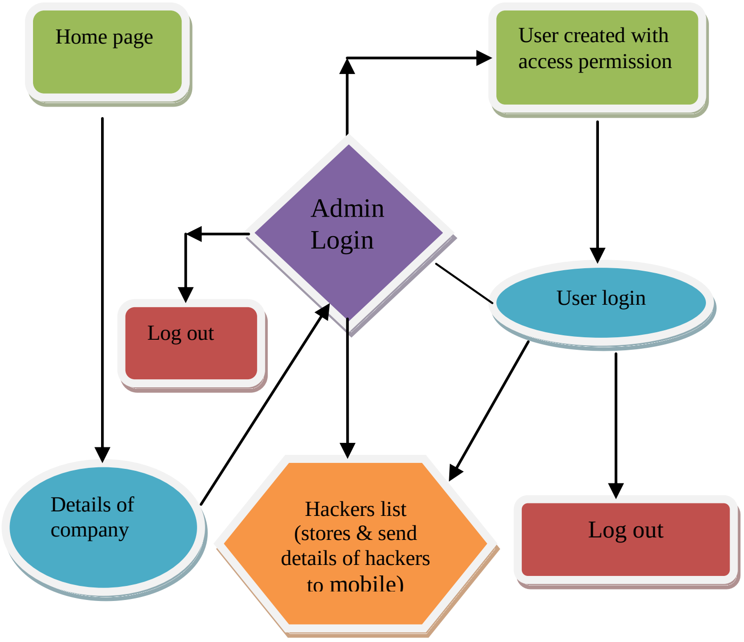
Home page
User created with access permission
Admin Login
Log out
User login
Details of company
Hackers list (stores & send details of hackers to mobile)
Log out

Figure 1.1 Flow Diagrams

In addition, greetings can be sent to friends. The user can view incoming mails and greetings. If anecdote of exploiter is being hacked with the purpose of possibilities searching the password by the plodder, then the user can view the hacker list details about the plodder with IP address in the respective user account. This method is similar to the method of dictionary attack.

Internet Protocol address is the one which contains a sequence of numbers, used to identify a particular computer or domain name on the Internet or Intranet. The two principal functions of IP address are host or network interface identification and location addressing.

II. RELATED WORK

There is a huge literature on third party emergency alert system over cellular networks. In Distributed Filtering for Internet services [1], Mayday emergency procedure is used. The client authentication and protocol verification is obtained as a result. The main drawback of the system is that the router architecture is found to be vulnerable.

In WebSOS: An Overlay-Based System for Protecting Web Servers from Denial of Service Attacks [4], the combination of graphic Turing test and cryptographic protocols are used. It allows authorized users to access a web server in the presence of a denial of service attack. Completion and long-term deployment of the WebSOS prototype on Planet Lab is not available.

In an Attack Causality in Internet-Connected Cellular Networks [7], the packet multiplexing is used. As a result, Robust Cellular Data Networks is obtained. Significant additional complexity and vulnerabilities occur in this system.

In Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks [6], Queue management and resource provisioning is used. Targeted text messaging attacks are eliminated. A problem occurs while dedicating the unused resources to the network

In Scalable Network-Layer Defence against Internet Bandwidth-Flooding Attacks [3], Active Internet Traffic Filtering (AITF) is used. As a result, it reduces the bandwidth flooding attack. It needs a few thousand filters and few MB of DRAM per client.

In Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services [13], Emergency Alert System (EAS) is used. Bulk messages are sent via Third Parties during emergencies. It is suitable only for smaller population and messages can be hacked.

III. WEBPAGE CREATION

The webpage is created for intranet mailing system. The company registration is done in this page. This company registration prompts the user to enter the company name. With the help of this company name, the user or the administrator can login into the company’s home page. The next field that is to be entered is the password which requests the user to enter the similar password twice to confirm the characters.

The address of the company has to be entered for the reference. The phone number field is the next field that is prompted to the user to enter. The website address of the company is then entered. The number of employees in the company is mentioned. The category of the company has to be entered.

In order to perform email routing, DNS and the server ID is entered. Once when the above details are entered, the registration is confirmed by clicking the save button. A maximum of three companies can be created. The registered companies will be displayed at the bottom of the webpage once they are created.

At the same time, the company login is given in the home page. It prompts for the company name and password that is given while registering the company. Once when the correct company name and the password are entered, login button is clicked so that it leads to the company's web page. Forgot password can be used when the password is being forgotten and it results in the recovery of the password.

User login is also available in the web page in which the username and the password have to be entered in order to view the home page of the user. The user registration or the user creation is done by the company administration in which the details are entered by the admin of the company.

IV. ACCOUNT AND MAIL MANAGEMENT

Account and mail management deals with the creation of user accounts and access permission given to the users. The company is registered and created in the home page. Created companies are viewed at the end of the home page. A particular company can be logged in so that it leads to the company's web page. The company's homepage involves,

i. Creation of the user
ii. Edit company information
iii. Managing mails.

A. Creation of the user

The employees in the company can create the user id so that the employees will be able to communicate via email. It prompts to enter the username. The availability of the username has to be checked once when the desired username is entered. The password is then entered and to confirm the entered password, user has to retype the password.

The photo of the user can be browsed from the system and it can be set. The personal information of the user has to be entered. It prompts the user to enter the first name, last name and the gender. The address for the communication is entered along with the country and the phone number. An alternate email ID is required which is meant to be optional. The security question along with the answer of that question has to be answered. This is done for the security purpose. Hacking of sms option is required. It can either be enabled or disabled according to the user's desirability. The registration of the user is now complete. If the hacking sms option is enabled during the user creation, only then the message is send to the user's mobile number during the hacking attacks. Similarly camera option is also provided to give better security for the users during login process.

After the completion of the creation of the user or the employee, the employee list that is created is displayed in the company's home page. Multiple employees can be created for a particular company and the list is displayed. Employee rights can be given to a particular employee. The employee is selected. The username and the password of the employee are mentioned. Compose rights, inbox rights and sent item rights are available.

Those rights to be given to a particular employee can be made enabled so that the employee enjoys all the rights that are given by the administrator. The above rights mean that the employee can compose the mail, send the mail to any user, and the sent mail is then saved in the sent item. The employee can modify the contents of the inbox and the sent item if the right is provided to the employee.

B, Edit Company Information

In this, the information of the company is edited. The username of the company can be edited along with the personal details that are entered during the registration or the creation of the company. In the user's home page, the user can compose the message and send to the desired user. The DNS and the server ID can be edited in the company information. The number of employees can also be edited. The account can also be deleted while editing the information of the company. This can be done by clicking edit company information.

In the user's home page, the account information and the personal information of a particular employee can be edited. While editing the account information the username along with the password can be changed. Also the security question that is given during the registration can be edited.

The personal information of the employee can also be edited. The first name and the last name of the user can be changed. Gender, address, phone number and the alternate email option can also be edited from the details that are entered during the creation of the account of an employee.

While composing the message in the 'to' field it is necessary to mention to whom the message has to be sent and in the subject field the description about the mail can be given. Also there is field as 'bcc' in which another user's mail ID can be mentioned so that the mail will be sent to the user that is mentioned in the bcc field. Hence the mail can be composed and sent to the multiple users.

In the same way, the sent mail can be viewed with the help of sent items in the account of the user. Once the mail is sent to any user, then immediately the mail will be saved in the sent item along with the details that to whom the mail is sent at what time and the date is also mentioned.

Once the mail is sent by the sender from his/her mail then the receiver will be able to view the mail that is sent by the sender. The receiver can then compose message if the employee right is applicable to the particular user.

C. Managing mails

E-Mail is the process of sending digital messages from a sender to one or more receivers. Postal communication may take more time. It may be completed in days or weeks to make the message available to others. But E-Mail services take lesser time to deliver the message to the recipients.

User's mail box is fully controlled by the administrator. The user can compose mail if the permission is given by the admin. Mail communication between the users of the registered companies is allowed. Deduction of spam mails module filter the mail that comes to the inbox. If the mail is found to be a malicious program, then the particular mail is stored in the spam. Deletion of mails is allowed to manage memory. User folder is an option provided to all the users. This option acts as a label and the users can move the important mails to this user folder.

V. MOBILE INDICATION HACKER LIST AND IP ADDRESS TRACKER

Mobile numbers which are entered during the registration of the user is used to send the text message when the user account is hacked. And also, hacking sms option should be turned on during registration to receive this alert message. The hacker may hack the user account by trying different possibilities. This kind of attack is said to be dictionary attack.

When an account is attempted for hacking, the hacker list is stored in the respective user account. The hacker list comprises of user name, password tried, date and time of attack and the IP address of the system from where the attack is made.

The company and the employees for each company are created. The company can be logged in with the particular company name and the password. Similarly, the user can log in with the particular username and the password created by the administrator.

While logging into the company login or into the user login, there might be chances of entering the wrong password. Also there may be possibilities of a wrong user to login with a wrong password. Once when the person tries to enter a wrong password with the username, then an indication will be sent to the mobile. At the same time the hacker list will be created in the user account.

The user identifies that the account is being hacked with the message that is sent to the mobile. Also when the user login the account with the correct username and the password, there will be an option as hacker list in the homepage of the user. If the user clicks the hacker list, then the list of hackers will be displayed. In that, the date and time of hacking will be shown. The passwords tried by the hacker will also be displayed.

With the hacker list displayed the user can track the IP address from which the particular account is hacked and will be able to find the hacker. This provides a greater security to the users from hacking.

VI. CONCLUSION

It is concluded that the system works well and satisfy the users. The system is tested very well in intranet. The hackers can bypass the web server to directly attack the server of the database. It is assumed that the attacks can neither be prevented nor detected by the current web server IDS, that hacker may take over the web server after the attack is over, and then later full control of the web server can be obtained to launch subsequent attacks. The site is simultaneously accessed from more than one system. Simultaneous login through intranet is tested. The site works according to the restrictions provided in their corresponding browsers.

In future the enhancements can be made to the application of the user, so that the web site functions very attractive and useful manner when compared to the present one. The speed of the transactions become more enough now. The security can also be given as per the requirement of the users. It also helps us to find the hacker in intrusions with the IP address.

ACKNOWLEDGMENT

Our Sincere thanks to our most respective Professor and Dean of the Department of Computer science and Engineering Dr.S.Karthik, Our beloved professor and Head of the Department Dr.T.KalaiKumaran and the people who are mainly motivate to prepare and publish this article in esteemed journal.

REFERENCES

[1] D. Andersen, “Mayday: Distributed Filtering for Internet Services,”Proc.USENIX Symp. Internet Technologies and Systems (USITS), 2003.

[2] T. Anderson, T. Roscoe, and D. Wetherall, “Preventing Internet Denial of Service with Capabilities,” Proc. ACM Workshop Hot Topics in Networking (HotNets), 2003.

[3] K. Argyraki and D.R. Cheriton, “Scalable Network-Layer Defense against Internet Bandwidth-Flooding Attacks,” ACM/IEEE Trans. Networking, vol. 17, no. 4, pp. 1284-1297, Aug. 2009.

[4] A. Stavrou, D.L. Cook, W.G. Morein, A.D. Keromytis, V. Misra, and D. Rubenstein, “WebSOS: An Overlay-Based System for Protecting Web Servers from Denial of Service Attacks,” J. Computer Networks, Special Issue on Web and Network Security, vol. 48, no. 5, pp. 781-807, 2005.

[5] A. Stavrou and A. Keromytis, “Countering DOS Attacks with Stateless Multipath Overlays,” Proc. ACM Conf. Computer and Comm. Security (CCS), 2005. P. Traynor, W. Enck, P. McDaniel, and T. La Porta, “Exploiting Open Functionality in SMS-Capable Cellular Networks,” J. Computer Security, vol. 16, no. 6, pp. 713-742, 2008.

[6] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, “Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks,” IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 40-53, Feb. 2009.

[7] P. Traynor, P. McDaniel, and T. La Porta, “On Attack Causality in Internet-Connected Cellular Networks,” Proc. USENIX Security Symp., 2007.

[8] TXTLaunchPad, “TXTLaunchPad Provides Bulk SMS Text Message Alerts,” http://www.txtlaunchpad.com, 2007.

[9] Voice shot, “Automated Emergency Alert Notification Call-VoiceShot,” http://www.voiceshot.com/public/urgentalert.asp?Ref=uaemergencyalert, 2008.

[10] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenkar, “DDoS Offense by Offense,” Proc. ACM SIGCOMM, 2006.

[11] Wikipedia, “Virginia Polytechnic Institute and State University,” http://en.wikipedia.org/wiki/Virginia_Tech, 2008.

[12] X. Yang, D. Wetherall, and T. Anderson, “TVA: A DoS-Limiting Network Architecture,” IEEE/ACM Trans. Networking (TON), vol. 16, no. 6, pp. 1267-1280, Dec. 2008.

[13] Patrick Traynor “Characterizing the Security Implications of Third-Party Emergency Alert Systems over Cellular Text Messaging Services” IEEE Transactions on Mobile Computing, Vol. 11, No. 6, June 2012.