International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 6, June 2014

A User Identity Management Protocol Using Efficient Dynamic Credentials

Sheetal S. Dharwadkar[1], **Rashmi M. Jogdand**[2]

[1]M.Tech Scholar, Gogte Institute of Technology and Engineering, Department of Computer Science and Engineering, Belgaum, Karnataka, India

[2]Gogte Institute of Technology and Engineering, Department of Computer Science and Engineering, Belgaum, Karnataka, India

Abstract: ***Today mobile devices make use of the services provided by the newly emerging technology Mobile Cloud Computing (MCC) to overcome the challenges of resource limitations such as, battery life, storage, computation power and bandwidth. Though this new technology is very flexible to use but however, the mobile devices are facing many challenges related to security. The legitimate users prove their identity to cloud using digital credentials such as passwords and digital certificate. As the technology has become very transparent adversaries may hack the valuable credentials of the user without the knowledge of legitimate user. The attackers may draw the services from cloud using the user's credentials and fool the cloud. The users will not come to know of this theft until some disaster has been done by the hacker. This system model proposes an light weight algorithm which reduces the burden of processing on mobile device as all computation are carried on trusted entity and it also improves the security of users Credentials by updating it dynamically based on the user and cloud communication.***

Keywords: Cloud Computing, Mobile cloud computing, Mobile devices, Credentials

1. Introduction

Recently the cloud computing technology has emerged as a new information technology infrastructure for the fast developing IT industry [1]. In cloud computing, information is permanently stored in large-scale data centers on the Internet all over the world and temporarily accessed and cached on clients including desktops and portable PCs, sensors, etc. With the "cloud" as a metaphor for the Internet, cloud computing promises to deliver massively scalable IT-enabled data, software, and hardware capabilities as a service to external clients with Internet accesses. And the highly scalable computation capability of the cloud data centers can further assist and accelerate most of our computation intensive services and works effectively. Therefore the cloud computing has been envisioned as the key technology to achieve economies of scale in the deployment and operation of IT solutions. Regarding recent advances in mobile communication technologies, it has made new revolution for all mobile user demands to experience rich mobile services [2]. Mobile users always expect broadband Internet access wherever they go, interact with each other via social networks while moving; furthermore, they are getting tremendous access to large sources of media-based contents and services. As the mobile devices are resource limited inherently, it is essential for the cloud to provide computational support for many media-rich applications. The combination of mobile media and cloud computing highly arises many technical challenges, and the main problem between resource consuming multimedia streams and power shortage of mobile devices has to be solved. Lots of effort is being made to provide worldwide rich experience of media on any screen which was not possible due to the heterogeneity among various mobile devices as they differ in physical factors, middleware platforms and interactive functions. Furthermore the developments of innovative pervasive mobile services, e.g., mobile video streaming, rich media dissemination, surveillance, gaming, e-health care, etc., can be greatly facilitated by mobile cloud computing platforms employing emerged and emerging technologies.

Few years ago a user was only expecting from mobile phone to perform common events like for e.g.: they usually used their personnel mobile phones to capture photos and store them on their mobile device local memory and use files which were stored on phone memory locally , but today due to the advancement in technologies around the world users are willing to make use of complex applications , external resources as storage area and computation power that are available outside the mobile phones .For achieving these types of performances a lot of changes have been carried out in several areas such as several improvements have been made in the areas such as mobile hardware and network . In spite of putting all efforts only little changes were made and mobile devices still have problem of storage resources and energy, an unstable connectivity and introduce several security issues.

Many a times, cloud computing is described as a list of services which are provided by an Internet-based cluster system which in turn consist of a group of low-cost servers or Personal Computers (PCs), organizing the various resources of the computers according to a certain management strategy, and offering safe, reliable, fast, convenient and transparent services such as data storage, accessing and computing to customers.

1.1 Mobile Cloud Computing

The combination of mobile devices and Cloud Computing services is known as Mobile Cloud Computing [2]. This new emerging technology has advantages to the mobile devices with low resources; advantages that lead to the development of rich functionality applications. Most applications which are developed for smart phones requires heavy computing power for executing heavy application and it also requires good software platform support . There are lots of problem with most low-end browser-enabled mobile phones to support such heavy applications of mobile devices. With the advancement in mobile cloud computing area, the resources in terms of computing power, storage area and platform support are all given by cloud for the execution of such applications.

Mobile Cloud Computing (MCC) today has become one of the industry buzz words and is a hot topic of discussion in the IT world since 2009, which combines mobile computing and cloud computing technology together [3]. The growth and advancement in the technology over last few in areas such as network based computing and applications on demand have made advancement in application models such as cloud computing, software as a service, community network, web store, and many more. Since from 2007 one of the main application model in the world of internet, cloud computing have become most interesting research topic of the scientific and industrial communities.

Today, smart phones which are connected to the Internet with the rapidly growing of wireless network technology are considered as the representative for the various mobile devices. Smart phones have two major features Ubiquity and mobility which in the next generation network will provide a range of personalized network services through numerous network terminals and modes of accessing. Centralizing computing is the core technology of cloud computing, very soon services and specific applications will become as a utility to be sold like water, gas or electricity to users. Now we can define, new computing mode, namely Mobile Cloud computes as the combination of a ubiquities mobile network and cloud computing.
Mobile cloud computing is inherited from cloud computing where the cloud computing networks are virtualized and assigned in a group of numerous distributed computers rather than in traditional local computers or servers, and are provided to mobile devices such as Smartphone's, portable terminal, and so on. Simultaneously there was lots of development of various application related to mobile cloud computing for example; Google's Gmail, Maps and Navigation systems for Mobile, Voice Search, and some applications on an Android platform, Mobile Me from Apple, Live Mesh from Microsoft, and MotoBlur from Motorola[4].

Mobile devices such as tablet, smart phones etc are becoming a very important part of all humans as the most easy and flexible communication way which is not restricted by time and place. There are a variety of services from mobile applications which the Mobile users can accumulate rich experiences (e.g., iPhone apps, Google apps, etc), these applications use wireless networks to run on the devices and/or on remote servers. There are many methods adopted in MCC for the movement of data in mobile environment [5].The data which switches between user and cloud is not in plain form it is protected from attackers by using various encryption and authentication methods [6]. The reason of the growth and development of entrepreneurs, commerce and IT industries is the rapid progress of mobile computing (MC) which has become a powerful trend in enhancement. Though this new technology is very flexible to use but however, the challenges mobile devices are facing due to their resources limitation are low battery, storage space, and bandwidth [7]. The improvement in the quality of services is hindered significantly by the limited resources of the mobile devices. Cloud computing (CC) is the technology that will be used widely as the next generation's computing infrastructure [1]. CC provides some advantages for users by allowing them to use infrastructure such as servers, networks, and storages devices as a service. CC provides another service called platforms such as operating systems as a service , and software as a service which gives application programs as a service which is provided by cloud providers such as (e.g., Google, Amazon, and Salesforce) at a very low cost. In addition, CC allows users to elastically utilize all resources from cloud in an on-demand fashion [8].There are many issues of security in CC which have been briefed out in [9] [10] [11]. In CC users are authenticated by using various methods which are discussed in [12] [13] before giving them full access rights.

As we know that CC provides a variety of services for mobile users and the use of mobile applications, we can say that mobile cloud computing (MCC) as an integration of cloud computing and mobile environment. MCC provides mobile users with new types of services and facilities for by which they can take full advantages of cloud [14].

1.2 Definition of Mobile Cloud Computing

"Mobile Cloud Computing is a technology, where both the data storage and the data processing do not take place in the mobile device but outside it inside the cloud. Mobile applications send the computing power and data storage out from mobile phones and move into the cloud, making possible that heavy applications can be used through smart phones ".

Though this technology is reaching to great heights there are many issues that need to be resolved related to privacy and security because of which this technology is still not being used by everyone in world[15][16][17]. Customers are hesitating to move their valuable to cloud because of the fear that it may be lost or stolen by opposite parties [18]. To solve these issues many solutions are provided in [19].

2. Existing System

Security is a critical issue for mobile cloud computing because all valuable information moves into the cloud of the mobile user. Among so many security issues a very important one is providing security to identities of users which are used by users to identify themselves in cloud. If an attacker is successful in faking credentials or stealing user credentials, such as passwords and digital certificates, then the user will be fooled and even cloud will be fooled by the attacker and the user will not come to know about this theft until some damage has taken place.

Until now only two algorithms have been implemented to provide security to users credentials by generating dynamic credentials.

1] Sheng Xiao and Weibo Gong [20] have proposed security scheme which identifies users in mobile environment .Usually digital credential methods are used such as passwords and digital certificate to identify the MU in mobile cloud environment. The security scheme proposed by these authors sees that the hacker does not impersonate the legal users and have proposed a light weight algorithm which generates automatic dynamic credentials. To generate dynamic credentials co-ordination among mobile user, manager and cloud service provider is very important. This algorithm discussed here generates dynamic credentials based on the user and cloud communication. Whenever messages are exchanged dynamic secrets are updated for cloud and mobile user. If Msg send is from mobile user then the dynamic secret of mobile user is updated by applying XOR operation on msg and mobile secret value as shown below

MU_Secret = Msg XOR MU_Secret ----------------------(1)

Now suppose the Msg is send by cloud then cloud dynamic secret are updated as shown below applying XOR operation.

CSP_Secret = Msg XOR CSP_Secret ---------------------(2)
Counter N is incremented for every dynamic secret update (N=N+1).

Dynamic credentials (D_Current) are generated when the user cloud communication reaches the threshold value which is decided by the user on how frequently he wants to update his credentials or when the user changes his data channel from base station to another. The credentials are updated bsed on the D_Current, MU_Secret, CSP_Secret as shown below

D_Current = D_Current XOR (MU_Secret || CSP_Secret)

The problem with this algorithm was firstly it considers cloud to be fully trusted to implement correctly. Second problem is that dynamic secret update for cloud and dynamic secret update for mobile user takes place on mobile device which increases the computing power and storage on mobile device.

2] Abdul Nasir Khan, et al [21] have tried to overcome some of the limitations which was found in the earlier algorithm proposed by Sheng Xiao and Weibo Gong .The proposed security algorithm generates dynamic credentials protect the user identity . The system model also works well in fully distrusted environment. This algorithm updates the dynamic credential when the user cloud communication reaches the threshold value or when the user wants to change the data channel from the base station. This proposed scheme has a trusted entity called as manager who is responsible for generating dynamic credentials , updating dynamic secret for cloud and updating dynamic secret for mobile user. Thus it reduces computation power and storage capacity on mobile device as all computation takes places by manager. The manager is trusted entity of the client organization. All communication between the cloud and user should take place through manager. Updating of dynamic secret for mobile user and cloud is done using same equation as shown above (1) and (2) . This model makes use of nonce to in increase the security. Nonce a random number is generated by manager separate for mobile user and cloud. This random number is used by manager to authenticate mobile user and cloud. Dynamic credentials are generated using mobile user secret, cloud secret and D_Current as shown in the equation above. The manger after generating the dynamic credentials sends it to the mobile user and cloud secretly using their nonce value so that if adversary by chance is able to eavesdrop the credentials he will not get because nonce are used.

3. Proposed System

The proposed system presents a light weight algorithm which generates dynamic credentials which acts as proof for identifying users in mobile cloud environment. This algorithm protects users from Man-Middle-Attack so that attacker will not be able to impersonate legitimate user and use users credentials for any wrong purpose. The credentials which are used for identifying users in MCC are passwords or digital certificate. Mobile devices are considered here as trusted entity and clouds are considered as fully distrusted entity. Manger entity is present in every client organization and is under the control of organization. The messages send by user first goes to manager and then from there manager forwards that message to cloud. Similarly messages send by cloud first goes to manager and then manager passes it to the user. All computation takes place at manager which overcomes the resource limitations of mobile devices and increases computation capacity and storage capacity at mobile device. To generate the dynamic secret for mobile user equation (1) is used and to generate the dynamic secret for cloud equation (2) is used. Dynamic credentials are generating using equation (3) when the user cloud communication as reached threshold value or when the user changes its data channel by requesting the base station. The threshold value is the number of packets and is decided by the user which is based upon how frequently he wants to update the credentials.

To provide security and make the algorithm stronger against the attackers this light weight algorithm uses nonce as well as threshing. By applying this it would be very difficult to the adversary to get the credentials.

```
def getDigest(Current_Credential):
digest = hashlib.sha256(Current_Credential).hexdigest()
for x in range(0, 100001):
digest = hashlib.sha256(digest).hexdigest()
return digest
```

In figure1, the user request is sent to the manager for authentication. In the next phase the manager generates dynamic credentials based on threshold value. Then cloud allows or denies download based on verification sent by manager.

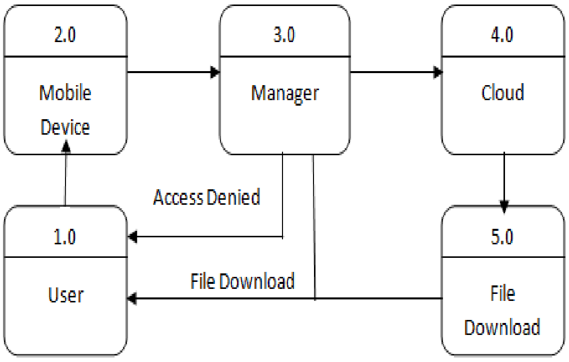

Figure 1: Communication between mobile device , Manager and CSP

3.1 Dynamic Credentials Distribution

Once the Dynamic credentials are generated next duty of the manger is to distribute it to mobile user and cloud. Manager first does the stretching on dynamic credentials generated. Passwords are usually stored using one of the two methods 1. plain text as original , or 2.it can be stored as the digest (output) which is result of one-way hash function. As we all know that passwords are very important credentials of users and it must be protected from hackers so storing credentials in plain text format will reveal easily the password to attackers whenever the users login, it would be better idea to adopt the second method to store the credentials of the users safely.

When we give the password as input to one way hash function one digest will be produced , now if we give this digest as input to one way hash function we get another digest, now let's create another digest from previous digest and one more digest from 3rd digest hence the last digest is the result of four iterations of hash function. Now we cannot create a digest from the password and compare it with the resulting digest, because the resulting digest is the result of the third digest, and the third digest is the result of the second digest. Hence if we want to compare passwords, same number of iterations needs to be made and then compare with the 4th digest. This is called stretching.

The manager combines nonce and the current dynamic credentials on which stretching is applied and then encrypts this concatenation by using public key of mobile device if the message is to be send to mobile user or encrypts this concatenation by using public key CSP if the message is to be send to CSP and then encrypts it using its private key which applies like digital signature and in this way sends the dynamic credentials to both mobile device and CSP.

3.2 Result and Analysis

3.2.1 Security Analysis

This algorithm makes the recovery of the current credential very tough as it is frequently updated whenever the communication reaches the threshold value. Let us assume that the attacker has the current credential at time t_0 and decides to attack at time $t_{1.}$ To make an attack at time t_1 he has to keep track of all communication between user and cloud to calculate value of current credential at t_1 . This is very difficult because of user mobility and unreliability of wireless communication but due to the advancements in technology the hacker may be successful in tracking the communication packets between cloud and user. After tracking the packets successfully between time t_0 and t_1 still the hacker will not be able to extract the value of dynamic credentials be in this scheme we have made use of nonce as well as stretching. Without the value of nonce attacker cannot get value of dynamic credentials. Even if the attacker is successful in getting the value of nonce but still he will not be able to recover the value of dynamic credentials as stretching is applied on credentials. Attacker may be successful in separating nonce and credential which is sent together in encrypted form by manager, but extracting credentials will become impossible because of stretching. By applying stretching the credentials value will be converted into digest that is the result of four iterations of the hash function. Guessing credentials using brute force method will become very long and impossible. Stretching makes this proposed system model very strong against Man-In-Middle attack and makes practically impossible for the hacker to recover dynamic credentials.

3.2.2 Performance Analysis

1]The graph in figure 2 shows that as the threshold value increases attacker gets time to hack and use credentials of mobile user. So as the threshold value increases the probability of attacking increases, if the threshold value is too small then dynamic credentials are generated frequently which makes system very slow ,therefore the threshold value should not be too less or too large hence in our system model we have taken optimal threshold value i.e. 5. By this the system performance becomes very efficient.

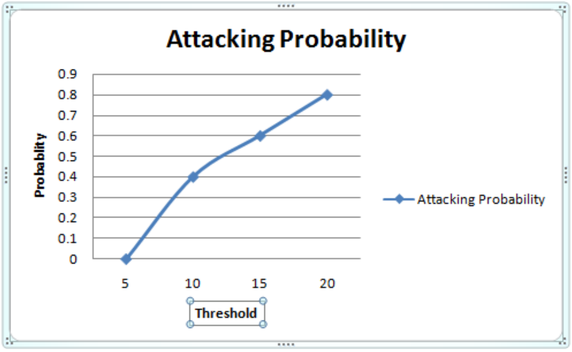

Figure 2 : Attacking Probability

2]In the graph in figure 3 from the readings it is clear that as the threshold value for dynamic credential generation increases the attack detection decreases because bigger the threshold value, the attacker has lot of chance to hack the mobile user's credentials. Thus attacks are more if there are many attacks simultaneously and hence attack detection decreases.

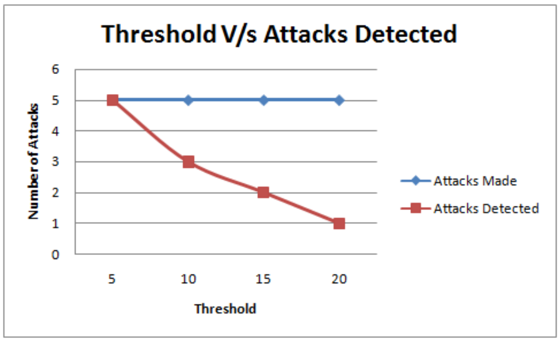

Figure 3 : Attack detection

4. Conclusion and Future Work

This system model proposes a light weight algorithm which generates dynamic credentials frequently and enhances the security of user credentials. The algorithm protects users against credentials robbery or fake credentials. The credentials are updated based on the user cloud packet exchanged. This scheme reduces Man-In-Middle attack as the algorithm is made stronger against this attack by using nonce and stretching. Even if the adversary is able to hack the credentials , he will not be able to extract it as we are using stretching and nonce methods. The users are authenticated by the manager before distributing the dynamic credentials. The user can also check whether the credentials received are not fake credentials by checking the digital signature.

A more detailed study can be done in area of generating dynamic credentials for user identity. Dynamic credentials scheme can be generated taking into consideration to reduce the processing burden on trusted entity and improve the systems overall scalability.

References

[1] Mohiuddin Ahmed, Abu Sina Md. Raju Chowdhury, Mustaq Ahmed, Md. Mahmudul Hasan Rafee. " An Advanced Survey on Cloud Computing and State-of-the-art Research Issues" . IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, ISSN (Online): 1694-0814, January 2012.

[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang. "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches". Accepted in Wireless Communications and Mobile Computing – Wiley

[3] Stuart Taylor, Andy Young, Neeraj Kumar, James Macaulay. "Mobile Consumers Reach for the Clouds". Cisco Internet Business Solutions Group (IBSG) ,July 2011.

[4] Dijiang Huang, Xinwen Zhang, Myong Kang, Jim Luo. " MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication", in: Proc. 5th IEEE Int. Symposium on Service Oriented System Engineering (SOSE '10), Nanjing, China, June 2010.

[5] Zhibin Zhou and Dijiang Huang. "Efficient and Secure Data Storage Operations for Mobile Cloud Computing", IACR Cryptology ePrint Archive: 185, 2011.

[6] John Bethencourt, Amit Sahai, Brent Waters . "Ciphertext-Policy Attribute-Based Encryption", in: Proc. 28th IEEE Symposium on Security and Privacy (SP '07), California, USA, May 2007.

[7] Abdul Nasir Khan a, M. L. Mat Kiaha, Sajjad A. Madanib, Atta ur Rehman Khana, Mazhar Ali." Towards secure mobile cloud computing: A survey". Future Generation Computer Systems 2012.

[8] Xinwen Zhang,Joshua Schiffman,Simon Gibbs, Anugeetha, Kunjithapatham,Sangoh Jeong. "Securing Elastic Applications on Mobile Devices for Cloud Computing". ACM 978-1-60558-784-4/09/11 Chicago, Illinois, USA ,November 13, 2009.

[9] Kuyoro S. O., Ibikunle F. & Awodele O. "Cloud Computing Security Issues and Challenges". International Journal of Computer Networks (IJCN), Volume (3) : Issue (5), 2011 .

[10] Mladen A. Vouk. "Cloud Computing – Issues,Research and Implementations". Journal of Computing and Information Technology - CIT 16, 235–246, 2008.

[11] Uttam Thakore. " Survey of Security Issues in Cloud Computing". College of Engineering, University of Florida.

[12] Safiriyu Eludiora, Olatunde Abiona, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawrence Kehinde." A User Identity Management Protocol for Cloud Computing Paradigm". Int. J. Communications, Network and System Sciences, 4, 152-163 March 2011.

[13] Shabnam Sharma, Usha Mittal. "Comparative Analysis Of Various Authentication Techniques In Cloud Comparative" . International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 4, ISSN: 2319-8753 April 2013.

[14] Swarnpreet Singh, Ritu Bagga, Devinder Singh, Tarun Jangwal. "Architecture Of Mobile Application, Security Issues And Services Involved In Mobile Cloud Computing Environment". International journal of computer and electronics research volume 1,ISSN : 2278-5795 August 2012.

[15] Manmohan Chaturvedi, Sapna Malik, Preeti Aggarwal and Shilpa Bahl. " Privacy & Security of Mobile Cloud Computing". Ansal University, Sector 55,Gurgaon-122011, India

[16] Soeung-Kon,Jung-Hoo,Sung Woo." Mobile Cloud Computing Security Considerations". Journal of Security Engineering April 30 2012.

[17] D. Popa,K. Boudaoud, M. Cremene M. Borda. "Overview on Mobile Cloud Computing Security Issues". Technical University of Cluj-Napoca, Communications Department,University of Nice Sophia Antipolis 2013.

[18] Jasleen . "Security Issues In Mobile Cloud Computing". Jasleen / International Journal of Computer Science &

Engineering Technology (IJCSET)ISSN : 2229-3345 Vol. 4 No, Phagwara, India ,July 2013.

[19] Markus Schüring. “Mobile cloud computing – open issues and solutions”. 15thTwente Student Conference on IT, Enschede, The Netherlands June 20th, 2011.

[20] Sheng Xiao and Weibo Gong. “Mobility Can Help: Protect User Identity with Dynamic Credential”, in: Proc. 11th Int. Conference on Mobile Data Management (MDM '10), Missouri, USA, May 2010.

[21] Abdul Nasir Khan a, M. L. Mat Kiaha, Sajjad A. Madanib, Atta ur Rehman Khana, Mazhar Ali.” Enhanced Dynamic Credentials Generation scheme for User Identity Protection in Mobile Cloud Computing”. Springer Journal, June 2013.

[22] Xinwen Zhang, Joshua Schiffman, Simon Gibbs,Anugeetha Kunjithapatham, and Sangoh Jeong. “Securing Elastic Applications on Mobile Devices for Cloud Computing”, in: Proc. ACM workshop on Cloud computing security (CCSW '09), Chicago, IL, USA, Nov. 2009.

[23] Monika Waghmare, Prof T.A.Chavan . “Outsourcing with secure accessibility in mobile cloud computing”. International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue4, April 2013.

[24] Manjulah.S , Manjunath A.E “Secure Data Processing Framework for Mobile Cloud Applications” International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6, June 2013.

[25] Song Wang, X. Sean Wang. “ In-Device Spatial Cloaking for Mobile User Privacy Assisted by the Cloud”, in: Proc. 11th Int. Conference on Mobile Data Management (MDM '10), Missouri, USA, May 2010.

[26] Dijiang Huang, Zhibin Zhou, Le Xu, Tianyi Xing, Yunji Zhong.” Secure Data Processing Framework for MobileCloud Computing”, in: Proc. IEEE INFOCOM Workshop on Cloud Computing (INFOCOM '11), Shanghai, China, June 2011.

[27] The RSA Algorithm Evgeny Milanov 3 June 2009 https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

Author Profile

PG M. Tech Scholar, Gogte Institute of Technology and Engineering, Belgaum, India. 8 Years of teaching Experience as Lecturer in Computer Science Department and Engineering, M. L. Bharatesh Polytechnic College, Belgaum, India. Interested in area of network Security.

Professor in Computer Science Department & Engineering, Gogte Institute of Technology and Engineering Belgaum, India. 21 Years of teaching experience, 6 years research work. Interested in area of Information security and network Security in Cloud Computing.