www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18730-18734

Performance of Multi Server Validation and Key Association with User Protection in Network Security

R. Padmini

Sri Padmavati Mahila Visvavidyalayam, School of Engineering and Technology,
Padmavati Nagar, Tirupati, Andhra Pradesh,INDIA
Padmini.rchandran@gmail.com

Abstract: ***The use of smart cards, far off person validation and key association can be simplified, bendy, and efficient for growing a comfy allotted computer systems surroundings. Addition to user authentication and key distribution, it is very useful for providing identification privacy for users. on this paper, we propose novel multi server authentication and key agreement schemes with consumer protection in community protection. We first endorse a single-server scheme and then observe this scheme to a multi-server environment. the principle deserves. Encompass: (1) The privacy of users may be ensured; (2) a consumer can freely choose his own password; (3) the computation and conversation price could be very low; (4) servers and users can authenticate every other; (five) it generates a consultation key agreed with the aid of the server and the person; (6) our proposed schemes are Nonce-based schemes which does now not have a serious time synchronization problem.***

Keywords: Network security, Privacy Protection, Session Key, Smart Card, User Authentication.

1. Introduction

For acquiring accredited offerings with the aid of carrier providers in an community surroundings, the person ought to legally login to the provider's server. In widespread, the user transmits a message of user authentication to the server, after which the server need to be able to affirm the identity of the consumer and give him the right of the use of approved services. Commonly, the user passes a password as a secret token to the server. The server first assessments if the person's identification and the password are matching. The server rejects the user's request if his identity or the password isn't always matching. If the password is matching, the server deliver the consumer the right for the usage of the accepted services. Lamport first proposed a password authentication scheme at the each ends of the conversation. for the reason that then, many schemes had been proposed to factor out its disadvantage and enhance the safety and efficiency of Lamport's scheme. best passing a password for authenticating between the user and the server isn't sufficient, for the reason that it is much less safety and is easily tapped by using the adversary. before two parties can do relaxed communique, a session key is needed for defensive subsequence communications. Also, the usage of smart playing cards, far off person authentication and key settlement may be simplified, bendy and green for creating a comfy allotted computers environment. it's also useful for providing identification privacy for the customers. Juang proposed two efficient validation and key association schemes for unmarried server, and multi-server environments. but each Juang's schemes haven't any capability of anonymity for the consumer. Yang et. al. Proposed user identification and key distribution scheme with the ability of privacy safety but we point out it's far much less efficient due to the use of public-key cryptosystems. For essentially safety and green requirements, the subsequent criteria are essential for far flung consumer authentication and key settlement schemes with clever cards.

2.AUTHENTICATION:

Once validation, association mechanisms control user access to appropriate gadget sources. Authorization can be labeled in step with the granularity of control; that is, according to how detailed a department is made between gadget resources. fine-grained authorization refers generically to a device wherein get entry to is managed to very quality increments, consisting of to individual programs or offerings. Authorization is frequently "role based totally" wherein get entry to to machine sources is primarily based on someone's assigned function in an agency. The gadget Administrator position might also have exceedingly privileged get admission to to all gadget sources whereas the well-known user function might best have get admission to a subset of those resources. Finer grained authorization may be carried out to outline other roles, which include Human resources directors role that has distinctive get entry to to personal HR databases, and an Accounting position that has specific get right of entry to to accounting systems. Validation may also be "rules based totally" whereby get entry to system sources is based totally on precise policies related to every user, independent of their role inside the company. For example, rules can be set up to permit study simplest get entry to or examine/Write access all or certain documents within a device, or access best at some stage in positive instances or from certain gadgets.

2.2. Authentication and authorization protocols : once validation, association mechanisms manipulate consumer get admission to suitable device sources. Authorization can be labeled in line with the granularity of manage; that is, in keeping with how particular a branch is made between device sources. High-quality-grained authorization refers generically to a tool in which get right of entry to is managed to very fine increments, consisting of two man or woman applications or services. Validation is regularly "position based absolutely"

wherein get admission to machine sources is based totally on someone's assigned characteristic in an organization. The system Administrator role may have highly privileged access to all machine sources while the fashionable consumer characteristic may excellent have get right of entry to to a subset of those sources. Finer grained authorization may be finished to outline other roles, which consist of a Human assets directors function that has one of a kind get entry to to personal HR databases, and an Accounting position that has unique get right of access to accounting systems. Validation may also be "policies based definitely" whereby access to system resources is primarily based mostly on unique rules related to every user, independent in their role in the employer. as an example, guidelines may be installation to permit look at simplest access or have a look at/Write get entry to all or certain files within a device numerous protocols had been normally adopted for authentication services. The RADIUS protocol is extensively used to centralize password authentication services. at the start designed to authenticate faraway dial-in users, the RADIUS protocol has been adopted for preferred consumer authentication offerings. Lately, the LDAP (light-weight directory get right of entry to protocol) has been finding enormous use in authentication and authorization structures. LDAP presents a convenient approach for storing person authentication and authorization credentials. RADIUS authentication servers are frequently coupled with credential storage in LDAP directories to provide centralized authentication and authorization. whilst a consumer attempts to access a particular application on this type of machine, the utility queries the user for authentication credentials and forwards them to the centralized gadget. The RADIUS server then tests the offered credentials towards those saved within the LDAP database, and additionally query the LDAP database for authorization rule statistics. The authentication effects (skip or fail) are returned to the software along with authorization rule information for the precise person. Authorization policies are then enforced on the utility to allow the user to access particular statistics or services. From an end-consumer perspective, those authentication and authorization structures ought to be automated and easy to use. e, or get entry to exceptional during nice times or from certain devices.

2.3. Validation and Association recommendations:

Nortel Networks recommends the following general principles to be followed when implementing enterprise authentication and authorization systems:

• Use a uniform access management system for end users, network operators, partners and customers, with the
Appropriate level of authentication and resource access authorization to meet business needs.

• Use a centralized authentication mechanism to facilitate administration and remove the need for locally stored passwords, which tend to be static and weak.

• Use a centralized authorization system, tightly coupled with validation system, with appropriate granularity for
the enterprise.

• Enforce strong, complex rules for all passwords.

• Securely store all passwords in one-way encrypted (hashed) format.

• Maintain simplicity to the extent appropriate, for maximum ease of use, ease of administration, and compliance.

• Securely log authentication and authorization events for audit purposes.

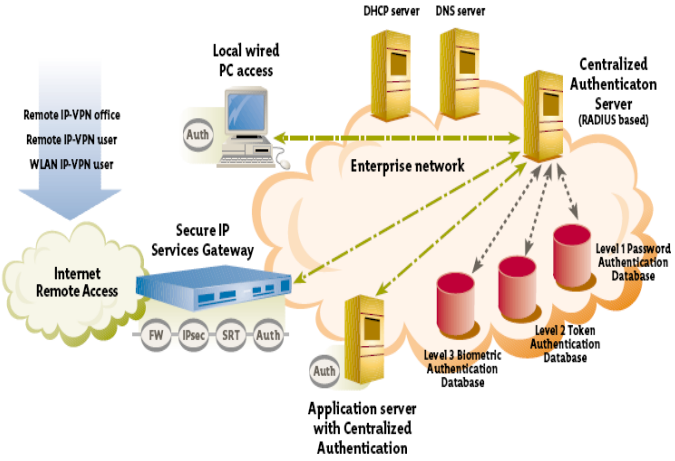

Fig: Secure validation and Association Reference model

3 NETWORK SECURITY IN THE REAL

This segment demonstrates this multi-stage safety Framework in motion for several actual-global situations:

• Securing the campus network
• Securing the records middle
• Securing the remote workplace

3.1. Securing the campus network:

In this context, the time period "campus" describes a company headquarters or huge nearby workplace where the network makes use of a mixture of technology, products, and packages, and serves a large consumer populace. The campus community presents a challenging security image because of the diversity of factors to protect:

•Servers, which includes departmental servers for user access and report sharing, valuable software servers along with finance and databases, and internet servers for either public internet or Intranet applications.

•Working systems, commonly multiple variations of more than one working systems going for walks on servers and customers.

•Community devices, along with routers, Layer four-7 load balancing switches, Layer three middle switches, Layer2 distribution switches, and Wi-Fi LAN get entry to factors.

•Protection gadgets, along with firewalls, VPN gateways, intrusion-detection and anti-virus servers, SSL accelerators, authentication servers, and content filtering servers.

3.2. Securing the data center:

The standard company records middle supports mission-important programs and houses a excessive attention of capital intensive sources and exclusive statistics—all linked to the inherently insecure internet as well as inner users. which means securing the records center provides a few precise necessities for failsafe safety without compromising performance and availability for users. The need will increase as organizations find out new approaches to exploit high-performance, internet-empowered information facilities:

• make certain commercial enterprise continuity. big processing throughput and transport bandwidth now make it feasible to save primary and copy units of essential statistics in more than one information facilities, in actual time—to extend

enterprise continuity offerings, real-time garage mirroring, and live backup across service issuer networks.

• Support crucial enterprise programs. businesses use information facilities to host commercial enterprise packages, implement firewalls or digital personal networks, provide garage offerings and content shipping of static and streaming media, and greater.

• Produce economies of scale on infrastructure. establishments can consolidate or outsource facts center functions, to centralize important computing assets, create virtual information facilities that span more than one locations, and decrease operational prices with out the overall performance penalty or safety issues normally related to faraway get right of entry to.

3.3. Securing the remote office:

The typical agency facts middle helps undertaking-important applications and homes a high concentration of capital
intensive assets and exclusive records—all connected to the inherently insecure internet as well as inner customers. which means securing the statistics center presents some specific requirements for failsafe security without compromising performance and availability for customers. The need will increase as organizations discover new approaches to make the most high-performance, internet-empowered facts centers:

• Make certain enterprise continuity. big processing throughput and shipping bandwidth now make it viable to
store number one and replica units of important records in more than one statistics facilities, in actual time—to extend business continuity
offerings, real-time garage mirroring, and live backup throughout carrier company networks.

• Assist crucial enterprise programs. enterprises use statistics centers to host commercial enterprise packages, enforce
firewalls or digital private networks, provide garage offerings and content delivery of static and streaming media,
and extra.

• Produce economies of scale on infrastructure. corporations can consolidate or outsource statistics middle features, to centralize vital computing assets, create virtual data centers that span more than one locations, and reduce operational charges with out the overall performance penalty or security concerns commonly associated with faraway get right of entry to.

4. NOTATIONS:

We first define the notation used on this paper. allow "X → Y: Z" denote that a sender X sends a message Z to a receiver Y , E ok(m) denote the cipher textual content of m encrypted the usage of the secret key okay of a few comfy symmetric cryptosystem , D okay(c) denote the plaintext of c decrypted the usage of the name of the game key k of the corresponding symmetric cryptosystem , "conventional string concatenation operator and ® denote the bitwise specific-or operator. let h be a public one-manner feature. Equations

4.1. Single Server Authentication Scheme:

In Juang proposed a user authentication and key settlement scheme the usage of smart playing cards with a lot much less computational price and more capability. The important drawbacks of this scheme are that it does now not provide the person anonymity functionality and it is not appropriate for multiserver environments. Allow S denote the server, U i denote consumer i. additionally, allow x be the secret key stored secretly with the aid of the server S. allow IDi be a unique identity of Ui. The scheme is as follows.

4.1.2. Registration segment:

Expect ui submits his identity IDi and his password PWi to the server for registration. If the server accepts this request, he's going to carry out the following i s secret information vi = h (Idi save IDi and wi to the reminiscence of a smart card and difficulty this smart card to Ui.

4. 1.3. Login and Session Key Agreement Phase:

After getting the shrewd card from the server, Ui can utilize it when he logins in the server. On the off chance that Ui needs to login to S, he should connect his savvy card to a card peruses. He then information sources his character IDi and his secret key PWi to this gadget. Accept that N1 is a nonce picked by Ui and N2 is a nonce picked by Sj for freshness checking. Expect that ruk is an arbitrary number picked by Ui and rsk is an irregular number picked by Sj for creating the session key ki = h(rsk||ruk||vi). The accompanying convention is the ith login regarding this savvy card.

convention is the ith login regarding this savvy card.

Step 1: Ui → S: N1, IDi,Evi (rui, h(IDi|| N1));

Step 2: S → Ui: Evi (rs,N1 + 1,N2);

Step 3: Ui→ S: Eki (N2 + 1).

4.2. Multi-Server Authentication Scheme:

Juang proposed a client verification and key assention plan utilizing brilliant cards for multi-server situations with considerably less computational expense and that's just the beginning usefulness. The real disadvantage of this plan is that it does not give the client secrecy usefulness. There are three sorts of members in this plan: clients, servers and an enlistment focus. In this plan, expect that the enlistment focus can be trusted. The enrollment focus looks at the legitimacy of login clients and after that issues a savvy card to qualified clients. The client just needs to enlist at the enlistment focus once and can utilize administrations gave by different servers. Let RC signify the enlistment focus, Sj mean server j, and Ui signify client i. Give UIDi a chance to be a one of a kind recognizable proof of Ui and SIDj be an interesting distinguishing proof of Sj . Likewise, let x be the mystery key kept subtly by RC, and wj = h

(x||SIDj) be the mystery key shared by Sj and RC. The common mystery key wj can be registered by RC and sent to Sj after he enlisted at RC. The proposed plan is as per the following.

4.2.2. Login and Session Key Agreement Phase:

In the wake of getting the shrewd card from RC, Ui can utilize it to login into Sj . Accept that N1 is a nonce picked by Ui and N2 is a nonce picked by Sj for freshness checking. Accept that ruk is an arbitrary number picked by Ui and rsk is an irregular number picked by Sj for creating the session key skk = h(rsk||ruk||vi,j). The accompanying convention is the kth login with admiration to his brilliant card.

Step 1: Ui → Sj : N1,UIDi,Evi,j (ruk, h(UIDi||N1));

Step 2: Sj → Ui : Evi,j (rsk,N1 + 1,N2);

Step 3: Ui → Sj : Eskk (N2 + 1)

4.2.3.Shared Key Inquiry Phase:

In Step 3 of the enrollment stage, RC will send the encoded shared mystery key Ewj (vi,j ,UIDi) to each Sj . After getting

the message, he will store it in his encoded shared key table. On the off chance that he don't need to control this table, the mutual key can be asked from RC when it is required. The accompanying convention can be embedded between Step 1 and Step 2 of the login and session key assention stage when Sj needs the mutual key.
Step 1': Sj → RC : N3,UIDi, SIDj ;
Step 1": Ewj (vi,j ,N3 + 1).

4.3. Client Authentication and Key Distribution Scheme :
Yang et al. proposed a client confirmation and key conveyance with client namelessness [21] in light of considering, discrete logarithm and hash capacities. The significant downsides of this plan are that it has a period synchronization issue, and the calculation and correspondence expense is still high. There are three sorts of members in this plan: a Smart Card Producing Center (SCPC), administration suppliers (servers) and clients. Let Ui indicate client i, Pj mean administration supplier j. This plan comprises of two stages: (1) the key era stage and (2) the mysterious client distinguishing proof stage. Their proposed plan is as per the following:

4.3.1. The key era stage:
The SCPC does the taking after to set up framework parameters.
1) Chooses two expansive primes p and q, processes n = pq, arbitrarily chooses a number e and processes d, where ed ≡ 1 mod Φ(n) and Φ (n) = (p − 1)(q − 1).
2) Chooses a component g ϵ Z* n which is a generator of both Z* p and Z* q .
3) Publishes (e, n, g) as open framework parameters and keeps (d, p, q) mystery.
4) Sends to each enrolled client Ui or administration supplier Pi a mystery token Si ≡ (IDi) d mod n, where IDi is The character of Ui or Pi. The unknown client distinguishing proof stage: If Ui needs to ask for an administration from Pj , they then plays out the accompanying strides:
Step 1: Ui Sends the administration solicitation to Pj for asking administrations from Pj .
Step 2: Upon accepting the solicitation, Pj picks an irregular number k and processes z ≡ g k S - 1 j mod n and sends z to Ui.
Step 3: Upon accepting z, Ui picks an irregular number what's more, does the accompanying calculations: a = z e ,IDj mod n, Kij = at mod n, x = g et mod n, s = g t Si h(x||T) mod n,
y = EKij (IDi), where T is the current timestamp and Ki,j is the normal session key. Ui then sends (x, s, y, T) to Pj .
Step 4: Upon accepting the message in Step 3, Pj checks the timestamp T . In the event that it is old, he prematurely ends the convention. Else, he then gets the basic session key Kij = xk mod n and afterward decodes y as IDi = DKij (y) and confirms xIDi h (x||T)?=se mod n. In the event that the check passes, then the administration solicitation is conceded.

5. SINGLE SERVER AUTHENTICATION AND KEY AGREEMENT WITH USER ANONYMITY:
In this segment, we propose a proficient single server client validation and key assention plan with security assurance. The idea utilized as a part of this segment will be utilized as a part of the following area to build a proficient multi-server client validation and key assention plan with security assurance. Give IDi a chance to be a one of a kind recognizable proof of client i. Moreover, give x a chance to be the expert mystery key kept subtly by the server S.

5.1. The Proposed Scheme
The proposed plan is as per the following.
5.1.1. Enlistment Phase: Ui
Accept Ui presents his personality IDi and his secret word PWi to the server S for enlistment. In the event that S acknowledges this solicitation, he will play out the accompanying strides:
Step 1: Compute Ui's mystery data αi = h(x||IDi) and βi = αi® PWi. Figure the pseudo recognizable proof number λi,1 = h(αi ||IDi||1) and records (k = 1, λi,1 , IDi) in a recognizable proof table
Step 2: Store IDi, λi,1, k = 1, and βi to the memory of a keen card and issue this shrewd card to Ui or send them subtly to Ui.
5.1.2. Client Authentication and Session Key Understanding Phase:
On the off chance that Ui needs to sign into S secretly, he should connect his keen card to a card peruser. He then sources of info his personality IDi also, his secret word PWi to this gadget. The accompanying convention is the kth login concerning this brilliant card.
Step 1: Ui → S : N1, λi,k ,E αi (ruk, h(N1||ruk|| λi,k));
Step 2: S → Ui : N2,E αi (rsk,h(rsk||N1||N2));
Step 3: Ui → S : Eskk (N2 + 1).

5.2.Execution Considerations:
We assess the productivity of our plan and Juang's plan . To begin with, we accept the square size of secure symmetric cryptosystems is 128 bits and the yield size of secure one way hashing capacities is 128 bits. Since both our proposed single-server plan and Juang's plan are in light of symmetric key cryptosystem, the execution is extremely well. In our plan and , the secret word length as it were 128 bits is required. Our proposed conspire needs 384 bits for the client confirmation. Both our own and Juang's plan [8], the calculation cost for enrollment is just required one hash operation. The calculation expense are amassed operation numbers,including encryption operations, unscrambling operations or hashing operations. The encryption what's more, encryption operations might be unbalanced or symmetric cryptosystem. In the login and session key assention stage of our plan, three symmetric key encryptions, three symmetric key decodings and seven hash operations are required. In that of Juang's plan , just three symmetric key encryptions, three symmetric key decodings and three hash operation are required. The calculation expense of the login and session key understanding is excluding expense of producing session key. Despite the fact that our proposed plan has somewhat high correspondence and calculation cost than Juang's plan , yet our plan have more finish usefulness.

6. MULTI-SERVER AUTHENTICATIONS Also, KEY AGREEMENT WITH USER
Namelessness: There are three sorts of members in our multi-server
convention: a key appropriation focus, administration suppliers (servers) and clients. Let KDC mean the trusted key dissemination focus, Ui indicate client i, Sj signify administration supplier j. Give UIDi a chance to be a one of a kind recognizable proof of Ui and SIDj be a novel recognizable proof of administration supplier j. Moreover, give x a chance to be the expert mystery key kept subtly by the key conveyance focus KDC and δj = h(x||SIDj) be the mystery key shared by Sj and KDC. The common mystery key δj can be processed by KDC and sent furtively to Sj after he enrolled at

KDC.

6.1.The Proposed Scheme:

The proposed plan is as per the following.

6.1.1. Enlistment Phase:

Accept Ui presents his character UIDi and his secret word PWi to KDC for enlistment. On the off chance that KDC acknowledges this solicitation, he will play out the accompanying strides: Compute Ui's mystery data _i = h(x || UIDi) what's more, _i = _i _ PWi.

7. CONCLUSIONS:

we have proposed two client validation and key understanding plans with security assurance for single server and multi-server situations. With respect to single-server plan, it is more basic and effective. With respect to multi-server plan, clients just need to enroll one time what's more, can utilize all gave administrations by administration suppliers. Both our proposed plans have the capacity of security insurance. Our plans additionally have low correspondence and calculation cost for client confirmation by just utilizing symmetric cryptosystems and one-way works. Likewise, our conspires effectively unravel the genuine time-synchronization issue in a conveyed PCs environment since our proposed plans are nonce-based.

REFERENCES

[1] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[2] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.

[3] Y. Chang and C. Chang, "Authentication schemes with no verification table," Applied Mathematics and Computation, vol. 167, pp. 820-832, 2005.

[4] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[5] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," Computers & Security, vol. 24, pp. 619-628, 2005.

[6] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authentication scheme," Mathematical and Computer Modelling, vol. 36, pp. 103-107, 2002.

[7] Mohan, P., & Thangavel, R. "Resource Selection in Grid Environment Based on Trust Evaluation using Feedback and Performance." American Journal of Applied Sciences, 10(8), 924-930. 2013.

[8] T. Hwang and W. Ku, "Repairable key distribution protocols for internet environments," IEEE Transactions on Communications, vol. 43, no. 5, pp. 1947-1950, 1995.

[9] W. Juang, "Efficient password authenticated key agreement using smart cards," Computers & Security, vol. 23, no. 2, pp. 167-173, 2004.

[10] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no.1, pp. 251-255, 2004.

[11] W. Juang and W. Nien, "Efficient password authenticated key agreement using bilinear pairings," in the 16th Information Security Conference, pp. 214-221,Taichung, Taiwan, June 2006.

[12] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, pp. 770-772, 1981.

[13] Annamalai, R., J. Srikanth, and M. Prakash. "Integrity and Privacy Sustenance of Shared Large Scale Images in the Cloud by Ring Signature." International Journal of Computer Applications 114.12, 2015.

[14] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B.Dodson, J. Hughes, and P. Leyland, "Factoring estimates for a 1024-bit RSA modulus," in Advances in Cryptology (Asiacrypt'03), LNCS 2894, pp. 55-74, Springer, New York, 2003.

[15] Prakash, M., & Ravichandran, T., "An Efficient Resource Selection and Binding Model for Job Scheduling in Grid." European Journal of Scientific Research, 81(4), 450-458, 2012.

[16] NIST FIPS PUB 197, Announcing the Advanced Encryption Standard (AES), National Institute of Standards and Technology, U. S. Department of Commerce, Nov. 2001.

[17] D. Seo and P. Sweeney, "Simple authenticated key agreement algorithm, Electronics Letters, vol. 35, pp. 1073-1074, 1999. ISSN : 0975-3397 1711

[18] M Prakash, R Farah Sayeed, S Princey, S Priyanka, "Deployment of MultiCloud Environment with Avoidance of DDOS Attack and Secured Data Privacy", International Journal of Applied Engineering Research, Vol 10, Issue 9, pp 8121-8124, 2015.

[19] C. Yang, T. Chang, and M. Hwang, "Cryptanalysis of simple authenticated key agreement protocols," IEICE Transactions on Fundamentals, vol. E87-A, no. 8, pp. 2174-2176, 2004.

[20] Annamalai, R., J. Srikanth, and M. Prakash. "Accessing the Data Efficiently using Prediction of Dynamic Data Algorithm." International Journal of Computer Applications 116.22 (2015).

[21] Y. Yang, S. Wang, F. Bao, J. Wang, and R. Deng, "New efficient user identification and key distribution scheme providing enhanced security," Computers and Security, vol. 23, no. 8, pp. 697-704, 2004.

[22] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767-782, May 2001.

Author Profile:

R. Padmini received the M.Tech Degree in Computer Science and Engineering from Siddarta Institute of Technology and Science , Assistant Professor, School of Engineering and Technology, SPMVV. She interest lies in the areas of Network Security, Computer Networks, Web Technologies, SQL, Data Mining.