Secure Authentication Scheme with Privacy Preservation Policy on Mobile Cloud Computing Environment

K. Naveen Prasad, K.R. Harsha Kashyap, KunalSutradhar, Tejas Kumar, S. Arun Kumar

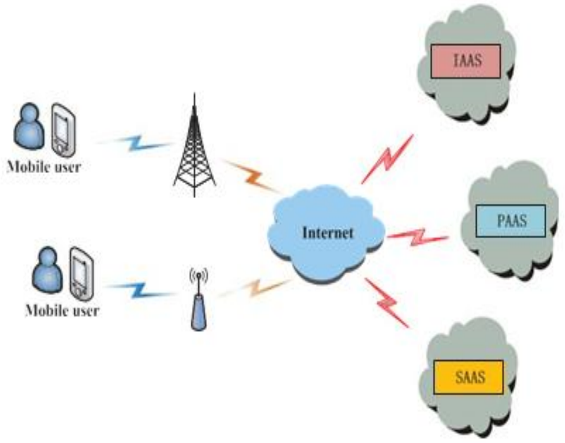
Abstract--- With the exponential augmentation of the mobile phones and the snappy headway of conveyed processing, another figuring perspective called compact disseminated registering (MCC) is progressed to unwind the confinement of the PDA's accumulating, correspondence, and count. Through mobile phones, customers can value diverse dispersed figuring organizations in the midst of their transportability. Nevertheless, it is difficult to ensure security and guarantee assurance because of the straightforwardness of remote correspondence in the new preparing perspective. Starting late, Tsai and Lo proposed a security careful approval (PAA) plan to deal with the conspicuous confirmation issue in MCC benefits and exhibited that their arrangement could contradict various sorts of existing attacks. Tragically, we found that Tsai and Lo's arrangement can't maintain a strategic distance from the expert association emulate strike, i.e., an adversary can copy the authority coop to the customer. Similarly, the adversary can isolate the customer's certified identity in the midst of executing the master center emulate strike. To address the above issues, in this paper, we manufacture another PAA scheme for MCC benefits by using a character based imprint plot. Security examination shows that the proposed PAA contrive can address the authentic security issues existing in Tsai and Lo's arrangement and can meet security essentials for MCC organizations. The execution appraisal shows that the proposed PAA scheme has less count and correspondence costs differentiated and Tsai and Lo's PAA plot.

List Terms--- CNN, DAP3D-Net, Computer Vision.

I. INTRODUCTION

Due to the deployment of wirelesscommunicationtechnologiesandthepopularityofmobiledevices(suchaslaptop,intelligentmobilephone,andtabletPC),wecanaccessthe Internet services during mobility. This bringsmuchconveniencetoourdailylifeaswecanenjoymanykindsofnetworkservicesanywhereandanytime.Withusers'increasingdemandof high services quality, a huge amount of data shouldbeprocessed in time by his/her mobile device. However,themobiledevices' resources (such as storage, computation,andcommunication capabilities) are limited and they cannotsatisfyusers'requirements[1]–[3].Thisweaknesshasbecomeaperformance bottleneck of various applications based on mobile devices.

In the past several years, the cloud computing developed rapidly as one of the powerful network technologies. Through the resource visualization technology, the cloud computing is able to provide convenient and cheap services to users' in a pay-as-you-go mode [4], [5]. For example, we can get some cloud storage services freely from many famous cloud ser- vice providers (CSPs) such as Baidu and Google. A new digital ecosystem called the mobile cloud computing (MCC) emergedrecently,wherethemobilecomputingisintegratedwith cloudcomputingplatforms.Withthisintegration,theresource-constrained problems of mobile devices could be addressed successfully.WiththeincreaseofMCCservices'types,thedistributedMCCisalsoemployedinpracticalapplications,where manykindsofCSPsareabletoprovidedifferenttypesofcloud services to users' [6], [7]. A typical architecture of MCC ser- vices is illustrated in Fig.1.



Because all the messages are transmitted by using the wire- less technology in MCC services environment, the adversary could control the communication channel easily, i.e., his/her is abletointercept,delay,andmodifytransmittedmessage.Then, the MCC services environment is more vulnerable to various types of attacks than traditional cloud computing services environment. To ensure that only the legal user can access MCC services and stop the adversary accessing MCC services, new securitymechanismsshouldbedevelopedfortheenvironment. The privacy-aware authentication (PAA) scheme is very crucialforaddresssecurityprobleminMCCservicesenvironment becauseitisabletoidentifytheparticipants'identitiesandprotect their privacy. Many PAA schemes have been proposed in the past several years.

Manuscript received June 10, 2019.

K. Naveen Prasad, SRM Institute of Science and Technology, Chennai, T.N, India.

K.R. HarshaKashyap, SRM Institute of Science and Technology, Chennai, T.N, India.

KunalSutradhar, SRM Institute of Science and Technology, Chennai, T.N, India

Tejas Kumar, SRM Institute of Science and Technology, Chennai, T.N, India

S. Arun Kumar, Assistant Professor, SRM Institute of Science and Technology, Chennai, T.N, India.

However, most of them are not suitable forMCCservicesbecausetheysufferserioussecurityproblem or have unsatisfactory performance. Therefore, it is necessary to designed new PAA schemes to ensure security and preserve privacy in MCC servicesenvironment.

To achieve mutual authentication (MA) in open networks, Lamport [8] proposedthe principal authentication scheme for the single server environment. In any case, Lamport's scheme can't avoid the replay attack and the impersonation attack. So as to improve security, several password-based authentication schemes are proposed [9]– [13]. Compared with Lam-port's scheme, those schemes have numerous focal points. Be that as it may, every server in those schemes needs to keep up a verifier table to achieve the MA. The enemy may mimic the client or the server when he/she takes verifier tables. Plus, those above schemes suffer from the disavowal of administration attack if the foe modifies the verifier table noxiously. To evacuate the genuine shortcomings, it is important to design authentication schemes with no verifier table.

Hwang and Li [14] planned the principal authentication scheme by utilizing both the password and the brilliant card. Contrasted and past authentication schemes [9]– [11], [15], [16], no verifier table is required in their scheme. In this manner, Hwang and Li's scheme has better security. To show signs of improvement execution, Sun [17] proposed an effective scheme dependent on Hwang and Li's work. Be that as it may, neither Hwang and Li's scheme [14] nor Sun's scheme [17] accomplish a MA. To accomplish better security and execution, numerous authentication schemes [18]– [25] utilizing both the password and the shrewd card were proposed in the most recent decades. Nonetheless, these schemes can't be straightforwardly utilized in MCC administrations condition on the grounds that numerous CSP exists in MCC administrations condition and the client needs to enroll in each CSP repeatedly. The client not just needs to put additional endeavors in recalling numerous passwords and identities yet in addition squanders a ton of time to execute repeated registration.

To understand the two weaknesses, the idea of the authentication scheme for the multi server condition was presented recently, where the client simply needs to enlist in the registration focus. Li et al. [26] proposed the main authentication scheme for the multi server condition. Notwithstanding, Lin et al. [27] brought up that the execution of their scheme isn't satisfactory because confounded neural systems are utilized to actualize the MA. To improve execution, Lin et al. [27] planned another scheme dependent on the discrete logarithm issue. Be that as it may, Cao and Zhong [28] brought up that Lin et al's. scheme [27] was uncertain against the pantomime assault. To improve performance further, a ton of such schemes [29]– [36] dependent on the symmetric cryptography were proposed to enhance security or performance.

In spite of the fact that the above schemes, utilizing the symmetric cryptosystem, have much preferable execution over past schemes, their security level isn't acceptable. For instance, they can't bolster the ideal forward mystery. To upgrade security and to improve the execution of these schemes, a few authentication schemes for multi-server conditions utilizing the elliptic bend cryptography (ECC) were proposed for practical applications. Yoon and Yoo [37] proposed such a scheme. Nonetheless, Yoon and Yoo'sscheme isn't verify at all on the grounds that a malicious client can mimic another client to get to administrations [38]. To upgrade security, He and Wang [39] exhibited an improved scheme utilizing ECC. Tragically, Odelu et al. [40] found that He and Wang's scheme was unreliable against two sorts of assaults and was not ready to give client anonymity. Along these lines, Odelu et al. [40] additionally displayed a security-improved scheme to address those issues.

The above schemes [37], [39], [40] have a few focal points than past schemes. However, they are not appropriate for MCC administrations in light of the fact that the registration focus ought to dependably be online to execute MA and it is pricey to build up a believed online registration focus. So as to address the issue, Tsai and Lo [41] proposed a PAA scheme for MCC administrations. Contrasted and past schemes [37], [39], [40], Tsai and Lo's scheme can secure client's protection and no online registration focus is expected to accomplish MA. Tsai and Lo [41] likewise demonstrated that their PAA scheme can oppose a ton of attacks. In this paper, we present a solid attack to demonstrate that their PAA scheme is shaky against the specialist co-op pantomime attack. In addition, we additionally demonstrate the enemy can get the client's genuine personality amid the execution of the above attack.

II. PROBLEM DESCRIPTION

The main problem in Mobile Cloud Computing

- How to ensure Security?
- How to protect Privacy?

Tsai and Lo proposed a privacy-aware authentication (PAA) scheme to overcome the above problem. The privacy-aware authentication (PAA) scheme is not able to solve one problem that is Service Provider Impersonation Attack.

To solve the above problem, we develop a NEW privacy-aware authentication (PAA) scheme for MCC services by using anIdentity-Based Signature Scheme.

Enhancement will work for multiple cloud Server. Tamper detection is possible. Mutual Authentication for Business to Business application.The main advantage is even if the attacker managed to compromise this shared secret somehow, it would only compromise that particular session.

III. PROPOSED MODELLING

In this paper, we focus on security and propose a novel information encryption approach. Our proposed methodology intends to specifically encode information and use protection order techniques under planning imperatives. This methodology is designed to amplify the security assurance scope by utilizing a particular encryption system inside the required execution time prerequisites.

This work proposes a novel methodology that specifically encodes information bundles to augment the security assurance level under planning limitations in enormous information.

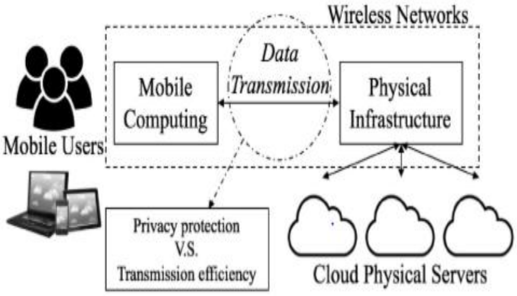
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Two working modes are viewed as while making the transmission methodology, including encryption and non-encryption modes.

Advantages:

- Classifying data packages according to privacy level.
- Determine whether data packages can be encrypted under the timing constraints.
- Encrypts data packages to maximize the privacy protection level under timing constraints.
- Provides the maximum value of total privacy weights
- Implemented in distributed storages in cloud computing

IV. SYSTEM ARCHITECTURE



In portable cloud computing, versatile system and cloud computing are joined, in this way giving ideal administrations to versatile customers. Cloud computing exists when assignments and information are kept on individual gadgets. Applications keep running on a remote server and after that sent to the customer. Here the mobile devices are connected to the mobile networks through the base stations; they will establish and control the connections (air interface) and functional interfaces between the mobile networks and mobile devices. Mobile users send service requests to the cloud through a web browser or desktop application.

The information's are transmitted to the centralprocessors that are connected to the servers providing mobile network services.

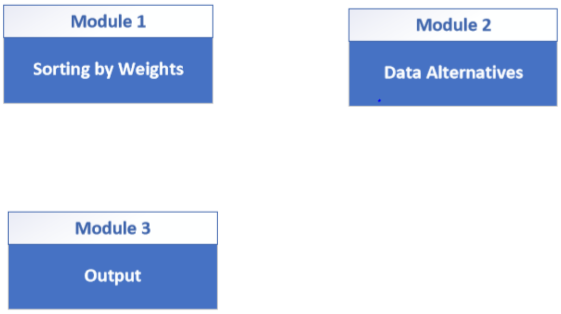
Here, services like AAA (Authentication, Authorization, and Accounting) can be provided to the users based on Home Agent (HA) and subscriber's data stored in databases.

A general architecture in a broader sense is presented in Fig.The subscribers‟ requests are then delivered to a cloudthrough the Internet. Cloud controllers present in thecloud, process the requests to furnish versatile clients with the comparing cloud administrations.

These administrations are created dependent on the ideas of utility processing, virtualization, and administration situated engineering.

The real capacity of a distributed computing framework is putting away information on the cloud and utilizing technology on the customer to get to that information. A few plans of action quickly developed to outfit this technology by giving programming applications, programming stages, information stockpiling, registering foundation and equipment as administrations.

V. MODULE DESCRIPTION



Module 1 Sorting by Weights

This is a preparation phase of the model. All data package types are sorted at this phase. The sorting operations consider both execution time and privacy protections; thus, two variables are involved, which are PWVs and the corresponding encryption execution time.

The next step is to map all sorting results into a table that is called S Table. The values of the sorting results can determine the priority.

Moreover, in order to improve the level of privacy protection, we introduce a Pairs Matching Collision (PMC) mechanism. This mechanism is designed to avoid the scenario when two plain texts can release users' privacy even though leaking each plain text will not be harmful.

The working rule of PMC mechanism is to ensure two pre-characterized pair information have something like one information encoded. The matched information must contain privacy data when they are transmitted or worked in plain messages. In view of the meaning of matched information, we propose a PMC mechanism to guarantee that somewhere around one information inside the combined information have the encryption need. Information transmissions in remote systems make an expansive number of chances for aggressors to intrude communications and take information. Privacy can be compromised even a few information sections are caught by foes on account of the propelled information mining techniques. In this paper, we build up a novel methodology that specifically encodes information so as to ensure privacy notwithstanding amid the information transmission process. The information encryptions rely upon the arrival estimation of the encryptions and information ascribes so as to limit the opportunity of privacy spillage when enemies apply information mining techniques.

Next, data alternatives are executed. Each encrypted data package's execution time is TeDi . We first encrypt the data package with the highest SDi value. The operation will not be ended until two situations occur. The first situation is that all data packages are encrypted. The other situation is that the execution time TeDi is longer than the rest of the time.

Define the rest of the execution time is Tr, where Tr<= Ts. In our model, we calculate time Tr considering both execution time with executions and execution time without encryptions.

Once the data package is selected to be encrypted, the execution time without encryption should be added to Tr. Assume that the selected data packages are {Ds}.

Module 2 Data Alternatives

This phase is the crucial step of selecting data packages for encryption operations. We propose the DED algorithm to accomplish this phase. S Table will be used for providing the reference of protection efficiencies. The operation will not be ended until two situations occur. The first situation is that all data packages are encrypted.

DED algorithm is designed to create the final privacy protection strategy corresponding with the timing constraints and security requirements.

The output is the data encryption strategy plan P that directs which data packages need to be encrypted. The crucial part of this algorithm is calculating the remainder of the available time so that the encryption strategy can be determined.

The main steps of DED algorithm are illustrated as follows:

- Input timing constraint Tc and two tables S Table and M Table. Initialize a strategy plan dataset P as an empty set. Initialize a variable endFlag and assign a False value to it.
- We use a While loop to create the strategy, which relies on the available time. We estimate whether the data packages should be encrypted one by one in a sequence depending on the priority weights. The data package having a higher-level priority will be determined first. Tm refers to the shortest execution time, which can be considered a total execution time without encryptions.
- Keep updating the execution time scope Ts. Each data package's non-encryption time needs to be added if the encryption time mode is selected during the process for updating the execution time scope.
- Add the data package to the set P when the value of Ts is greater than 0 and the encryption time of certain data package is no longer than Ts. This process follows the principle that higher priority weight goes first.
- End while loop when there is no data package matching the condition any more. 6. Output the set P that consists of a set of data packages Di. Encrypt all data packages in p.

Module 3 Output &Analytical Results

This phase mainly output an encryption plan deriving from the outcomes of Phase II. Those data with higher-level encryption priority will be selected for the encryptions under a certain constraints. The rest of data will not be encrypted such that plain texts operations are applied.

The WM algorithm is developed for modifying M Table using weight values. The purpose of this algorithm is to check whether a data package is a must-encrypted objective, when considering the relations between packages. Thus, the pairs matching collisions are applied in this algorithm in order to detect the paired data. Inputs include an M Table and a CoTable. The output of this algorithm is a modified M Table, which is represented as an MTable'. A Co-Table refers to a table mapping all paired data, which is predefined by security policies or developers. The Co-Table is used to manipulate pairs matching collisions.

The main phases of Algorithm 5.2 include:

- Input the original mapping table M Table and the predefined Co-Table.
- For all data Di in M Table, determine whether data Di is involved in table Co-Table. Find out the paired data Dj when Di is in Co-Table and this pairing process is represented as Di <->Dj .
- Judge whether data Dj is in the mapping table M Table in order to determine whether the weight value needs to be modified. The weight value needs to be changed when Dj is in M Table.
- Compare the encryption time lengths between Di and Dj . Assign an infinity value to DeDi when the execution time Di is shorter than D'j s. Otherwise, assign an infinity value to DeDj , which means that we consider this data the highest encryption priority.
- After all data are operated and updated, output the modified table M-Table'.

VI. SOFTWARE REQUIREMENTS

To implement the project we do some requirements that are used to build the task. So to perform the functionality of the project we use language Python as a back-end and HTML,CSS,JavaScript as front-end using algorithm Perfect Forward Secrecy and we use a platform called Liclipse software and to store the data generated we use Structured Query Language, SQL database.

VII. CONCLUSION

Because of the profoundly powerful nature of cell phones in the MCC environment, the conventional authentication schemes are not appropriate for different administrations in this environment. To take care of the security issue in MCC administrations, Tsai and Lo proposed an efficient PAA scheme for the MCC benefits by utilizing the bilinear blending. This paper calls attention to that Tsai and Lo's PAA scheme is vulnerable to a genuine assault and can't bolster client anonymity. To fathom such genuine weaknesses, the paper proposes another PAA scheme for MCC administrations. Security examination demonstrates that our proposed PAA scheme can take care of the security issue existing in Tsai and Lo's PAA scheme. In addition, the performance investigation demonstrates that our proposed PAA scheme has preferred performance over their PAA scheme. Later on, we will investigate more attributes of the proposed scheme, which can be connected for secure administration access in MCC environment.

REFERENCES

1. M. Satyanarayanan, "Fundamental challenges in mobile computing," in*Proc. 15th Annu. ACM Symp. Princ. Distrib. Comput.*, 1996, pp. 1–7.

2. Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, “Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud datasupporting parallel computing,” *IEICE Trans. Commun.*, vol. 98, no. 1, pp. 190–200, 2015.
3. Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi- keyword ranked search scheme over encrypted cloud data,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Feb. 2016.
4. M. Armbrust*et al.*, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.
5. A. Lin and N.-C. Chen, “Cloud computing as an innovation: Percepetion, attitude, and adoption,” *Int. J. Inf. Manag.*, vol. 32, no. 6, pp. 533–540, 2012.
6. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.
7. Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, “Mutual verifiable provable data auditing in public cloud storage,” *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015.
8. L. Lamport, “Password authentication with insecure communication,”*Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.
9. E.-J. Yoon, K.-Y. Yoo, C. Kim, Y.-S. Hong, M. Jo, and H.-H. Chen, “A secure and efficient sip authentication scheme for converged VOIP networks,” *Comput. Commun.*, vol. 33, no. 14, pp. 1674–1681, 2010.
10. R. Arshad and N. Ikram, “Elliptic curve cryptography based mutual au- thentication scheme for session initiation protocol,” *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 165–178, 2013.
11. S. H. Islam and G. Biswas, “Design of improved password authentication and update scheme based on elliptic curve cryptography,” *Math. Comput. Modelling*, vol. 57, no. 11, pp. 2703–2717, 2013.
12. P. Guo, J. Wang, X. Geng, S. K. Chang, and J.-U. Kim, “A variable threshold-value authentication architecture for wireless mesh networks,”*J. Internet Technol.*, vol. 15, no. 6, pp. 929–935, 2014.
13. J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, “A novel routing protocol providing good transmission reliability in underwater sensor networks,”*J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.
14. M.-S. Hwang and L.-H. Li, “A new remote user authentication scheme using smart cards,” *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28– 30, Feb. 2000.
15. M. S. Farash and M. A. Attari, “An anonymous and untraceable password- based authentication scheme for session initiation protocol using smart cards,” *Int. J. Commun. Syst.*, vol. 29, no. 13, pp. 1956–1967, 2016.
16. A. Irshad, M. Sher, M. S. Faisal, A. Ghani, M. Ul Hassan, and S. Ashraf Ch, “A secure authentication scheme for session initiation protocol by using ECC on the basis of the tang and LIU scheme,” *Secur. Commun. Netw.*, vol. 7, no. 8, pp. 1210–1218, 2014.
17. H.-M. Sun, “An efficient remote use authentication scheme using smart cards,” *IEEE Trans. Consum. Electron.*, vol. 46, no. 4, pp. 958–961, Nov. 2000.
18. J.-L. Tsai, T.-C. Wu, and K.-Y. Tsai, “New dynamic ID authentication scheme using smart cards,” *Int. J. Commun. Syst.*, vol. 23, no. 12, pp. 1449– 1462, 2010.
19. C.-T. Li, C.-C. Lee, and C.-W. Lee, “An improved two-factor user au- thentication protocol for wireless sensor networks using elliptic curve cryptography,” *Sensor Lett.*, vol. 11, no. 5, pp. 958–965, 2013.
20. S. H. Islam and G. Biswas, “Dynamic ID-based remote user mutual au- thentication scheme with smartcard using elliptic curve cryptography,” *J. Electron.*, vol. 31, no. 5, pp. 473–488, 2014.
21. M. S. Farash, S. Kumari, and M. Bakhtiari, “Cryptanalysis and improve- ment of a robust smart card secured authentication scheme on SIP us- ing elliptic curve cryptography,” *Multimedia Tools Appl.*, vol. 75, no. 8, pp. 4485–4504, 2016.
22. C.-L. Hsu, Y.-H. Chuang, and C.-l. Kuo, “A novel remote user authentica- tion scheme from bilinear pairings via internet,” *Wireless Pers. Commun.*, vol. 83, no. 1, pp. 163–174, 2015.
23. A. Irshad, M. Sher, E. Rehman, S. A. Ch, M. U. Hassan, and A. Ghani, “A single round-trip sip authentication scheme for voice over internet protocol using smart card,” *Multimedia Tools Appl.*, vol. 74, no. 11, pp. 3967–3984, 2015.
24. A. K. Das, “A secure and robust password-based remote user authentica- tion scheme using smart cards for the integrated EPR information system,” *J. Med. Syst.*, vol. 39, no. 3, pp. 1–14, 2015.
25. D. Mishra, “On the security flaws in id-based password authentication schemes for telecare medical information systems,” *J. Med. Syst.*, vol. 39, no. 1, pp. 1–16, 2015.
26. L.-H. Li, L.-C. Lin, and M.-S. Hwang, “A remote password authentication scheme for multiserver architecture using neural networks,” *IEEE Trans. Neural Netw.*, vol. 12, no. 6, pp. 1498–1504, Nov. 2001.
27. I.-C. Lin, M.-S. Hwang, and L.-H. Li, “A new remote user authentica- tion scheme for multi-server architecture,” *Future Gener. Comput. Syst.*, vol. 19, no. 1, pp. 13–22,2003.
28. X.CaoandS.Zhong,“Breakingaremoteuserauthenticationscheme for multi-server architecture,” *IEEE Commun. Lett.*, vol. 10, no. 8, pp. 580– 581, Aug.2006.
29. C.-C. Lee, T.-H. Lin, and R.-X. Chang, “A secure dynamic ID based remote user authentication scheme for multi-server environment using smartcards,”*ExpertSyst.Appl.*,vol.38,no.11,pp.13863–13870,2011.
30. S. K. Sood, A. K. Sarje, and K. Singh, “A secure dynamic identity based authentication protocol for multi-server architecture,” *J. Netw. Comput. Appl.*, vol. 34, no. 2, pp. 609–618,2011.
31. X. Li, Y. Xiong, J. Ma, and W. Wang, “An efficient and security dy- namic identity based authentication protocol for multi-serverarchitecture using smart cards,” *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 763–769, 2012.
32. W.-J.Tsaur,J.-H.Li,andW.-B.Lee,“Anefficientandsecuremulti-server authenticationschemewithkeyagreement,”*J.Syst.Softw.*,vol.85,no.4, pp. 876–882,2012.
33. K. Xue, P. Hong, and C. Ma, “A lightweight dynamic pseudonym iden- tity based authentication and key agreement protocol without verification tables for multi-server architecture,” *J. Comput. Syst. Sci.*, vol. 80, no. 1, pp. 195–206,2014.
34. D.Mishra,A.K.Das,andS.Mukhopadhyay,“Asecureuseranonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards,” *Expert Syst. Appl.*, vol. 41, no. 18, pp.8129– 8143,2014.
35. X. Li, J. Niu, S. Kumari, J. Liao, and W. Liang, “An enhancement of a smart card authentication scheme for multi-server architecture,”*Wireless Pers. Commun.*, vol. 80, no. 1, pp. 175–192,2015.
36. S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy, “Secure and efficient smart-card-based remote user authentication scheme for multi-serverenvironment,”*Can.J.Electr.Comput.Eng.*,vol.38,no.1,pp.20–30,2015.E.-J. Yoon and K.-Y. Yoo, “Robust biometrics-based multi-serverauthen- tication with key agreement scheme for smart cards on elliptic curve cryptosystem,” *J. Supercomput.*, vol. 63, no. 1, pp. 235–255,2013.
37. H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, “Cryptanalysis and im- provement of a biometrics-based multi-server authentication with keyagreementscheme,”in*Proc.Int.Conf.Comput.Sci.Appl.*,2012,pp. 391– 406.