Journal of Engineering and Applied Sciences 14 (4): 1189-1197, 2019
ISSN: 1816-949X

Enhanced TPUA Mechanism with Data Protection Using ID in Cloud Computing

[1]K. Sujatha and [2]V. Ceronmani Sharmila
[1]Department of Computer Science and Engineering,
[2]Department of Information Technology, Hindustan University,
603103 Padur, India

Abstract: User authentication is the core element which offers authentication, authorization and accounting in cloud computing environments for cloud users. In recent years, so, many authentication schemes for cloud computing has been introduced. Either the authentication scheme involves security problems or cannot be implemented in the cloud computing environment. The proposed system, TPUA that is Two Phase User Authentication mechanism using ID is easily adapted to a cloud computing environment and deals with the security problems spotted in related authentication schemes. It involves user authentication which provides complete mutual authentication with data protection. When compared to other user authentication schemes the proposed system has higher security and minimal computational costs.

Key words: User authentication, cloud computing, TPUA, cryptography, computing environment, cloud

INTRODUCTION

Cloud computing is the internet based computing. The process is storage and access to the data and programs over the internet instead of our computer hard drive. The cloud is a model to enable on demand services with the pool of computing resources. It can be one of the following types: public cloud is publicly accessible services and accessed over the internet. A private cloud is private services which are deployed on private networks and it is managed by third parties. Hybrid cloud is a combination of both public and private services.

The cloud based system described by the following attributes. Multi-tenancy represents the sharing of resources to the consumers, host and application level by service providers. Massive scalability is the ability to scale bandwidth, storage and systems. Elasticity represents the number of resources can be increased or decreased as per the requirement. Pay-as-you-go is the advantage for the consumers, so, they can pay the resources which they consumed. Self-provisioning of resouces are known as the consumers have the ability to select the resources.

Now a days cloud computing forms the revolution in data storage and processing mechanisms. It enables the following on demand services. Software as a Service (SaaS) where the software is deployed over the internet and designed for end users. Platform as a Service (PaaS) is a computing platform which allows the creation of web applications using a set of tools and software. Infrastructure as a Service (IaaS) is a complete cloud computing infrastructure delivery consists of servers, storage, networks and operating system.

The cloud services are categorized by the SPI service model. It represents the different levels and layers of service that can be available to end users by service providers over the different application domains and types of cloud. Clouds can be used to offer as-a-service like as-a-software to use as-a-platform to develop onand as-as-a infrastructure to develop.

Software as-a-service: It represents the application that is deployed over a cloud. These are the applications which offer an API to allow for greater application extensibility.

Platform as-a-service: It represents a platform of development in which the developers can use to write, deploy and manage application that run on the cloud.

Infrastructure as-a-service: It offers the developers to use the infrastructure to run the applications. It can be comprised of storage, virtual servers, database and other things. Figure 1 represents the overall view of the SPI (SaaS, PaaS, IaaS) service model.

The cloud offers services for consumers including storage for data, ensuring application and data processing that is of real time. The consumers can remotely store the data into the cloud and they can avail the scalable services.

Corresponding Author: K. Sujatha, Department of Computer Science and Engineering, Hindustan University, 603103 Padur, India

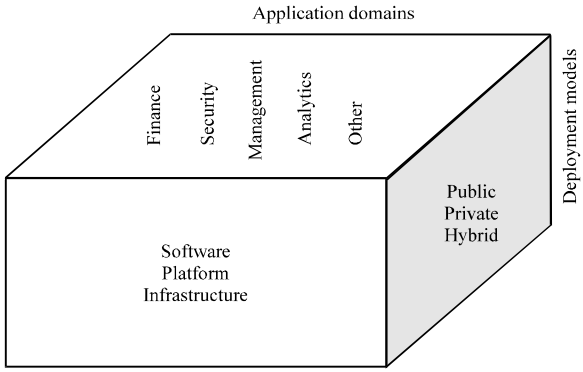

Fig. 1: SPI service model

A cloud service includes infrastructures, storage over the internet and delivery of software. Cloud computing becomes trending research topics citing the above grounds stated. User authentication schemes are critical in the cloud which offers authorization to the end user and server in order to maintain confidentiality.

The major challenges in cloud computing involve privacy and security because of its multitenancy nature and the subcontracting of infrastructure. Authentication is generally referred to as a process that ensures the user identity and the rights to the system. A basic method of authentication (Menkus, 1988) involves the following procedures.

- Some information a person knows (for example, password, personal ID)
- Some information a person possess (for example, token, card)
- Some information a person involves (for example, history of internet usage)
- Something a person is (for example, fingerprint, voice)

Recent authentication trends in cloud computing (Ramgovind *et al*., 2010; Carolan *et al*., 2009) involve authentication frameworks, architectures and models, passwords and smart card based authentication and biometric authentication methods.

Normally cloud computing issues will be broadly classified into two classes. They are service provider encountering problems and customer encountering problems. Some of the threats in cloud computing are data breaches, weak identity insecure API, malicious insiders, data loss, denial of service, shared technology issues, system and application vulnerabilities.

Above said threats could be avoided if one adopts authentication mechanisms such as working of authentication on a private network, identity management, authentication techniques.

Data protection in the cloud is a type of data protection model which used to protect data while in cloud server and data transmission. It is designed to ensure secure data storage, protection and security methodologies.

Some existing authentication techniques are password based authentication, two factor authentication, multifactor authentication, single sign on, key stroke analysis, graphical authentication, user authentication by smart cards, shared authority based authentication. The cloud data protection provides and ensures various services and processes such as:

Integrity: It is a basic component of information security. It refers to the accuracy and consistency of data stored in the cloud server.

Storage management: Data protection model is intended to save the log activities and file entries.

Infrastructure security: These are the set of policies and measures that ensures the security of the cloud/storage infrastructure.

Backup: It can be considered as the most fundamental and important concept in data protection. It offers data protection by creating duplicate copies of the original copy. Data protection model offers backup services to regulate and simplify the process of routine backups. It is easy to replicate the files in the local system.

Recovery: It is normally linked with backup which serves as a recovery solution in case the production copy gets lost. Data protection model supports easy and quick browsing and recovery not only for specific files but also entire systems.

Disaster recovery: It is the recovery of complete vital IT infrastructure at a remote site when the production site becomes unavailable. It saves the loss of productivity and reputation.

High availability: It provides effective failover protection against hardware and operating system. It is based on failover processing, backup, data storage and access. Data protection model ensures fault-tolerant systems streamlined for high availability.

To provide flawless security with data protection in a cloud computing environment the focusing elements are mutual authentication between end users and cloud server, security and efficiency with low computation and communication cost.

Literature review: In this study, some of the related researches to the proposed mechanism has been reviewed. Das *et al.* (2004) proposed a scheme for user authentication using smart cards. They have incorporated dynamic ID in the scheme which protects the identity of the user. It competes against stolen verifier attacks because of the absence of verifier table. It withstands some of the security breaches such as guessing attacks forgery attacks and replay attacks. Anyhow, this scheme does not provide any security against impersonation attack and random password attack.

Yang *et al.* (2008) proposed an improved scheme for user authentication using smart card in a multi server environment. Though this scheme can combats against several attacks, further research shows that it still lacks in complete security. This scheme does not withstand against impersonation attack and message alteration attack.

Lee *et al.* (2009) pointed out that Wang's scheme still has some security flaws and it does not ensure complete mutual authentication. To overcome the security flaws they proposed improvised version of that scheme which is highly efficient and secure. However, still it is susceptible when the smart card is stolen and by the malicious server.

Hsiang and Shih (2009) proposed a new scheme based on Wang's scheme which introduces the concept of session key with mutual authentication. But every client in the environment must know the server's identity. In reality it does not sounds for a better implementation.

Above mentioned schemes are discussing the security flaws either in a single server environment or a multi server environment. More over these schemes are having high computation costs and not focusing the situations of cloud computing environments.

Moghaddam *et al.* (2014) introduces the concept of agent for authentication in cloud computing. Client side user authentication agent is responsible for ensuring client identity. For storage of data in the cloud cryptography agent is used. This scheme increases the reliability and trustworthiness in cloud computing. But it suffers in the computational cost.

Zhen *et al.* proposed an improvised version of ID based user authentication with key agreement. Still facing some security flaws and challenging computational cost.

According to strong authentication scheme (Choudhury *et al.*, 2011) which provides mutual authentication between end users and cloud server with a unique ID for each registration and session key for each communication to avoid replay attack. This cloud architecture has seven steps:

- Step 1: Inserts smart card and enters user's unique ID and PWD
- Step 2: Depends on user's information, validation takes place by the local system and the request is forwarded to the cloud server
- Step 3: The cloud server replied to that request with some data based on user information
- Step 4: One time key is sent to the mobile network by the cloud server
- Step 5: The user gets one time key from the mobile network
- Step 6: Server authentication takes place by the user based on ID, password and smart card and forwards the message to the server
- Step 7: Finally, the last step of mutual authentication takes place at the side of the server

This strong user authentication mechanism can avoid several popular attacks like DoS attack, MITM attack, stolen verifier attack and phishing attack.

Yang *et al.* (2013) and Chen *et al.* (2013) introduces ID based scheme. Though it has several security advantages still lacks in efficiency and computational costs moreover, these schemes do not support data protection as addressed in cryptanalysis of ID based remote user authentication scheme (Ahmed *et al.*, 2009). Though it has several security advantages still lacks in efficiency and computational costs.

Hajivali *et al.* (2013) discussed about applying agent for user authentication and access controls. This scheme is reliable, secure in a cloud computing environment. But the factor, efficiency is still not in balance because by implementing more agents in the process which leads to high cost of communication and computation.

Zhang and Zhang (2015) and Mo *et al.* (2016) were discussed about user authentication in a cloud computing environment using the intermediate trusted centre. But these schemes do not support the data protection.

Even though above mentioned schemes are introduced in cloud computing environments still having some security breaches with high computational costs in user authentication.

Focusing on these problems, the proposed system provides two phase authentication without smart cards in cloud computing environments. The first phase includes authorization and mutual authentication by IDI between

end users and cloud server. The second phase, IDI involves authentication of users while data transmission and dual encryption on data which is stored in cloud server.

The proposed scheme uses simple exclusive OR functions and single way hash function. So that, computational costs are highly reduced. It increases the security and strongly commands about mutual authentication. Finally, the proposed scheme provides efficient and secure two phase user authentication mechanism with data protection using ID for cloud computing.

MATERIALS AND METHODS

In related research, all the process will take place in between end user and server. In the proposed scheme, IDI which is identity issuer is introduced for end users and server authorization and leads to mutual authentication. It does not maintain any verification table that leads to avoid stolen verifier attacks. In first phase IDI involves mutual authentication between cloud server and end users. Figure 2 represents the overall view of the phase I user authentication.

Authorization

Step 1: The user sends ID-EU and ID-S to the IDI.

Step 2: The IDI computes the hash function of user Id with secret value and sends the computed value UA to the user. Then IDI computes the hash function of UA and sends to the server. Figure 3 represents the process of IDI in the authorization.

Mutual authentication: The following steps show that the process of mutual authentication between the end users and cloud server.

Step 1: The user chooses a random number RU and then computes the hash function of UA, server ID and TS.

Step 2: The server checks TS. If it is not valid then the server denies.

Step 3: If it is valid then server computes RU and Hash function of RU. If it matches, then the server allows. Otherwise, the server denies the user.

Step 4: The server computes hash function of ID of user and server and timestamp with secret value and random number which is selected by the server. It sends to the user.

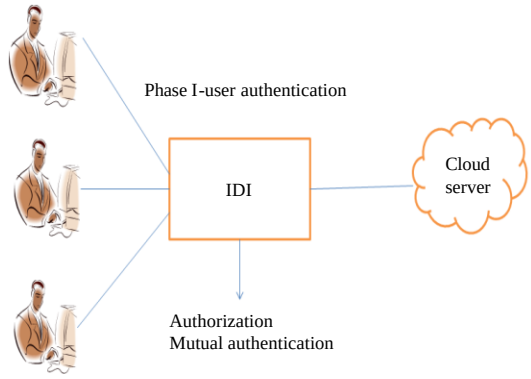

Fig. 2: Phase I user authentication

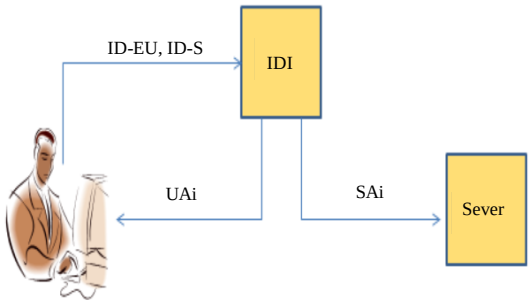

Fig. 3: Authorization

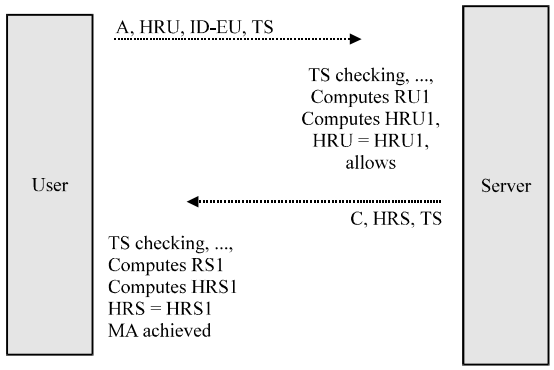

Fig. 4: Mutual authentication

Step 5: The user checks the TS. If it is valid the user computes the same hash function and checks with the received, if they are equal then the user ensures the server is legal. By implementing 3rd and 5th step in the process will proceed to the mutual authentication between end user and cloud server.

The proposed scheme involves the functions of single-way hash functions and exclusive OR operations. It improves higher security and reduces computation costs. The proposed ystem can be adapted to multi server environments because of the computed value UA which is offered by the ID Issuer (IDI). Figure 4 shows the process of mutual authentication between end user and cloud server.

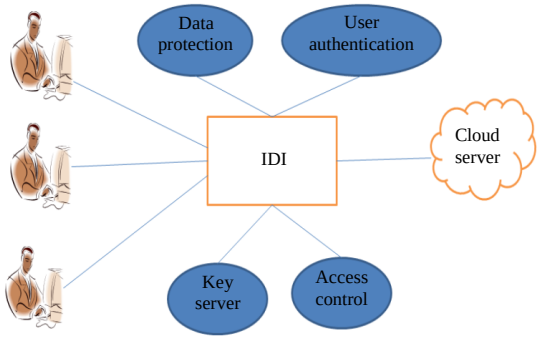

Fig. 5: Data protection (Phase 2)

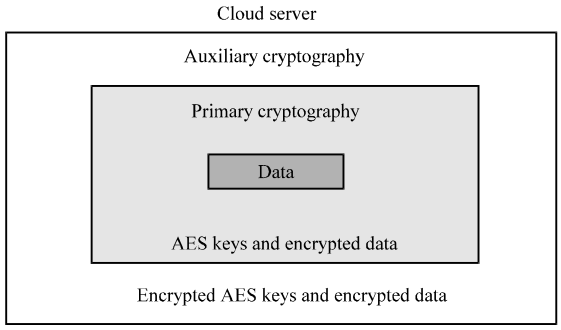

Fig. 6: Two levels of encryption in cloud server

In the second phase, IDI involves data protection which leads to two levels of encryption on data stored in cloud server. The responsibility of IDI in the second phase are data protection, user authentication, key server and access control.

In the data protection, IDI is responsible for dual encryption on data which stored in cloud server. In the user authentication, IDI again checks the identity of the end users. Key server is responsible for maintaining private and public keys of user and data for auxiliary encryption. In access control data are travelled in encrypted form to ensure the security. Figure 5 represents the overall view of phase II user authentication which includes data protection.

In the data protection, the primary cryptography ensures the security of the data in cloud servers. This encryption works with the concept of AES because symmetric encryption is most suitable in the first level.

In the auxiliary cryptography establishes the second phase of user authentication and data protection to cloud server. The key of primary cryptography is re-encrypted with RSA to protect the procedure of primary cryptography. Figure 6 shows the levels of encryption performed by IDI on data which is stored in the cloud server.

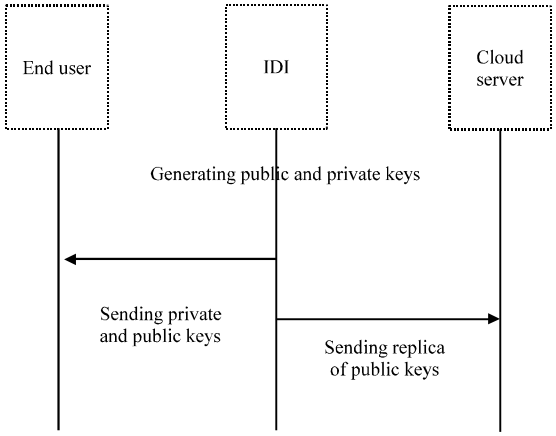

Fig. 7: Key server

In phase 2, there are some responsibility for IDI to implement data protection are key server, user authentication and access control.

Key server: While in the process of dual encryption to achieve the data protection, all the keys are generated and stored in IDI and it is used whenever needed.

For the auxiliary cryptography the public keys and private keys are generated in IDI. The private keys and public keys are sent to the user and the replicas of the public keys sent to the cloud server. Figure 7 represents the sequence of key generation and distribution by IDI.

User authentication: If the end user is the applicant of data then he can send request for data by encrypting the request using the private key of its own. IDI will decrypt the request by the user's public key and verifies the user's identity.

If the end user is the owner of the data then, the encrypted request from the data applicant is sent to the owner through the IDI. On the data owner side, the verification is encrypted initially by its own private key and then the private key of data. Now the encrypted verification is sent to the IDI. IDI will decrypt the encrypted verification by the public key of the data owner. Moreover, the verification is stored in the storage of IDI to maintain log entries which leads higher security in access control.

Figure 8 represents the sequence of the authentication process between end users those can be either data owner and data applicant and IDI.

Access control: To access the data, IDI will encrypt the private key of data with a user's private key. This encrypted key is sent to the cloud server. On the other

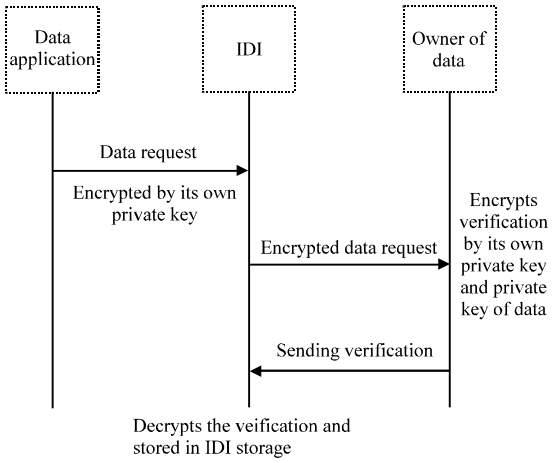

Fig. 8: Sequence of user authentication

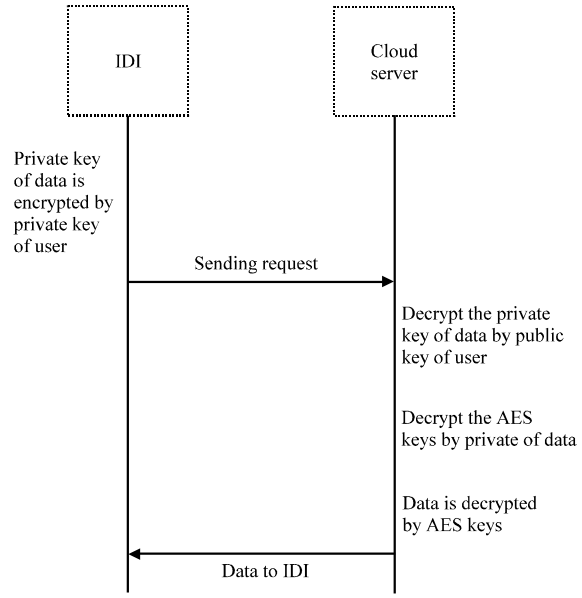

Fig. 9: Access control

side, the cloud server will decrypt the key by the public key of the user. Now, the cloud server will get the private key of data. By using the private key of data the AES main keys are decrypted. By using the AES keys the data in cloud storage will be decrypted. Then the decrypted data will be sent to the IDI. By the way, the access controls are protected by IDI. Figure 9 represents the procedure of access control.

By using effective intermediate middleware like IDI in data protection, user authentication and access control will obviously enhance the reliability, efficiency, trustworthiness and high security in the cloud computing environment.

In real time, the proposed system is suitable for cloud computing environment with more secure, highly efficient with reduced computational cost. Moreover, it provides data protection which resolves more security flaws and increases rate of trust.

RESULTS AND DISCUSSION

Evaluation of proposed scheme: The proposed system implemented by node JS in server side, front end by angular, MongoDB for storage and uses the AWS cloud computing environment. The proposed syatem involves the AWS cloud products for security such as Amazon Cognito Amazon GuardDuty Amazon Identity and Access Management and Amazon Inspector. Amazon Cognito involves in user sign-up and user sign-in. It adds the user sign-up, user sign-in and access control to the web and mobile applicationseasily and quickly.

Amazon GuardDuty is used for threat detection service. It is a managed threat detection service which provides accurate and easy way for protection and monitor the AWS accounts and workloads. AWS Identity and Access Management (IAM) is used for access control. It involves in user access control to AWS services. It is used to create and manage users and groups and grant access or deny access. Amazon Inspector involves in the security assessment. It is an automated security assessment. This automated security assessment service which helps to improve the security and compliance of applications deployed on AWS. Figure 10 and 11 shows some of the implementation sequence. The following parameters are considered important criteria to evaluate the proposed scheme:

Efficiency: The authentication process in the proposed scheme has been very efficient by implementing IDI between end users and cloud server. Accordingly, each user has to confirm their identity twice to the server initially and at the time of data transmission.

On the basis of theoretical analysis, the performance analysis of the related works has given in Table 1. The computation cost is the combination of XOR function and a single way hash function. Table 2 shows that the performance analysis of proposed scheme which clearly states the low computational costs compared to the related schemes.

Figure 12 shows the performance analysis of the proposed scheme with related works. According to graph which is evidence that the computational costs of the proposed scheme are less than those of Wang *et al.*'s scheme and Das *et al.* (2004) scheme in the user and server sides. Thus, the proposed scheme is more efficient than the related works for cloud computing.

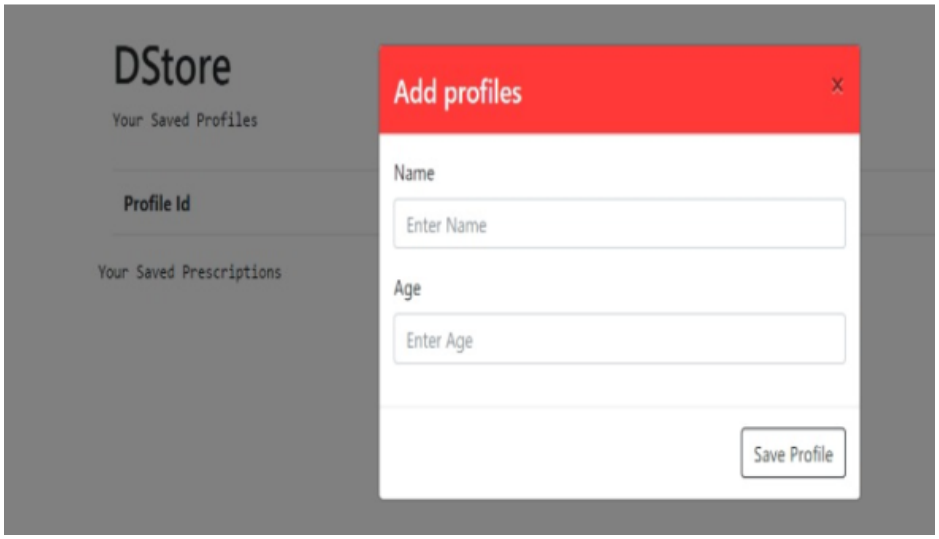

Fig. 10: Storage implementation

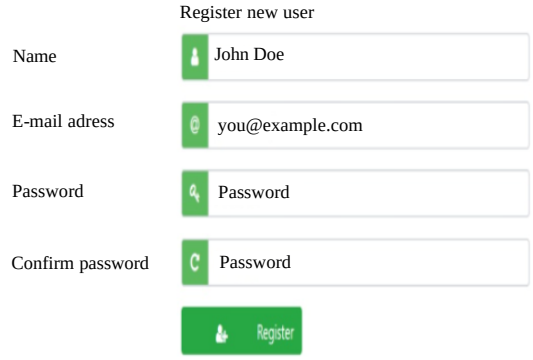

Fig. 11: User registration

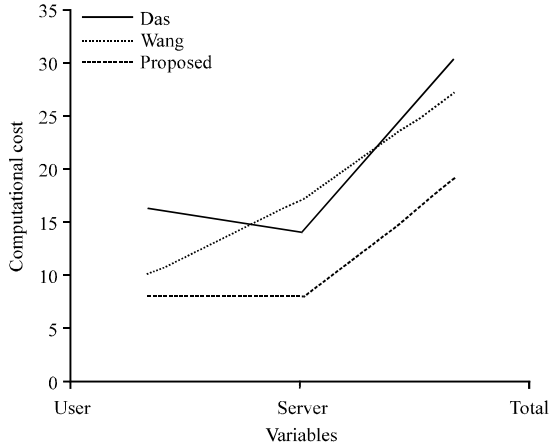

Fig. 12: Performance graph

Security: By implementing two phase authentication of end users and dual encryption on data which is stored in cloud server enormously enhances the rate of trust in a cloud computing environment. We can analyze some of the security threats with the related schemes to the proposed scheme. Table 3 shows that the comparison of related scheme with proposed TPUA using the ID.

Table 1: Performance analysis of related works

	Proposed scheme		
Function	User	Server	IDI
XOR operation	4	4	1
Hash function	4	4	2
Computation costs	4XOR+4H	4XOR+4H	1XOR+2H
Total	9XOR+10H		

Table 2: Performance analysis of proposed scheme

	Das *et al.*'s scheme		Wang *et al.*'s scheme	
Function/related scheme	User	Server	User	Server
XOR Operation	9	8	6	10
Hash function	7	6	4	7
Computation costs	9XOR+7H	8X0R+6H	6X0R+4H	10X0R+7H
Total	17XOR+13H	16X0R+11H		

Table 3: Comparison of related works

Scheme/functionality	Das *et al.* (2004)	Liao *et al.* (2006)	Chueh and Sun (2017)	Proposed
Mutual authentication	No	Partial	Yes	Yes
Stolen verifier attack	Yes	Yes	Yes	Yes
Message alteration	No	No	No	Yes
Impersonation attack	No	No	Yes	Yes
Computational cost	High	High	High	Low

Yes: the attack is resolved by the scheme; No: the attack is not resolved by the scheme

Mutual authentication: In the 3rd step of mutual authentication the user checks whether the computed HRU1 is matches the received HRU. Subsequently in the 5th step server checks the authenticated user by computed HRS. Hence, mutual authentication is achieved between end users and cloud server.

Stolen verifier attack: In the proposed scheme, the server and IDI does not store any verification table because it is completely dependent on random numbers which is generated every time on both server and client side while authentication and data transmission. So that, stolen verifier attack is not possible.

Replay attack: Consider that an attacker hacks the log in-request message and re-sends to the server. The server identifies the request malicious because the log in request message contains A which is the manipulation of Random number RU and Time Stamp TS which are keep on changing every time. So that, the replay attack is impossible in the proposed scheme.

Password based attacks: In the proposed scheme end users does not have any password based authentication, so that, there is no need for password change and no need to consider a password guessing attack.

Phishing attacks: Mutual authentication is performed between the end user and cloud server by IDI. So, only the genuine server can send the verification message HRS and which will be verified by the user. So that, the proposed scheme is strong against the phishing attacks.

Reliability: By using dual encryption on data which is stored in cloud server will enhances the reliability of the system. If any one of the cryptographic algorithm fails the security of the system is guaranteed by the other cryptography. By this, the reliability and efficiency of the system enhance significantly.

CONCLUSION

The proposed scheme that is TPUA mechanism using ID in cloud computing which allows mutual authentication between end users and server. Along with mutual authentication IDI involves data protection on data which is stored in cloud server. By employing IDI to the system that provides highly efficient, trustworthy and suitable scheme for cloud computing environment. The proposed system eliminates the important security breaches because of dual encryption performed in data protection and has low computational costs.

NOTATIONS

ID-EU = End User Identity
ID-S = Server Identity
SH(.) = Single way Hash Function
TS = Time Stamp
X = Server's secret value
RU = Random number selected by User
RS = Random number selected by the Server
(XOR) = Exclusive OR
UA = Authentication message to User
SA = Authentication message to Server

REFERENCES

Ahmed, M.A., D.R. Lakshmi and S.S. Sattar, 2009. Cryptanalysis of a more efficient and secure dynamic ID-based remote user authentication scheme. Intl. J. Netw. Secur. Appl., 1: 32-37.

Carolan, J., S. Gaede, J. Baty, G. Brunette and A. Licht *et al*., 2009. Introduction to Cloud Computing Architecture. 1st Edn., Micro Systems Inc, ýMenlo Park, Californiaý, USA.,.

Chen, P.L., J.H. Yang and C.I. Lin, 2013. ID-Based user authentication scheme for cloud computing. J. Electron. Sci. Technol., 11: 221-224.

Choudhury, A.J., P. Kumar, M. Sain, H. Lim and H. Jae-Lee, 2011. A strong user authentication framework for cloud computing. Proceedings of the 2011 IEEE International Conference on Asia-Pacific Services Computing (APSCC), December 12-15, 2011, IEEE, Jeju Island, South Korea, ISBN:978-1-4673-0206-7, pp: 110-115.

Chueh, J.S. and M.T. Sun, 2017. Design and implementation of security system for cloud storage. Proceedings of the 2017 19th International Symposium on Asia-Pacific Network Operations and Management (APNOMS), September 27-29, 2017, IEEE, Seoul, South Korea, ISBN:978-1-5386-1102-9, pp: 129-134.

Das, M.L., A. Saxena and V.P. Gulati, 2004. A dynamic id-based remote user authentication scheme. IEEE Trans. Consumer Elect., 50: 629-631.

Hajivali, M., F.F. Moghaddam, M.T. Alrashdan and A.Z. Alothmani, 2013. Applying an agent-based user authentication and access control model for cloud servers. Proceedings of the 2013 International Conference on ICT Convergence (ICTC), October 14-16, 2013, IEEE, Jeju, South Korea, ISBN:978-1-4799-0698-7, pp: 807-812.

Hsiang, H.C. and W.K. Shih, 2009. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Comput. Stand. Interf., 31: 1118-1123.

Lee, H., D. Choi, Y. Lee, D. Won and S. Kim, 2009. Security weaknesses of dynamic ID-based remote user authentication protocol. Proce. World Acad. Sci. Eng. Technol., 59: 190-193.

Liao, I.E., C.C. Lee and M.S. Hwang, 2006. A password authentication scheme over insecure networks. J. Comput. Syst. Sci., 72: 727-740.

Menkus, B., 1988. Understanding the use of passwords. Comput. Secur., 7: 132-136.

Mo, J., Z. Hu and Y. Lin, 2016. A user authentication scheme based on trusted platform for cloud computing. Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, November 16-18, 2016, Springer, Cham, ISBN:978-3-319-49147-9, pp: 122-130.

Moghaddam, F.F., S.G. Moghaddam, S. Rouzbeh, S.K. Araghi and N.M. Alibeigi *et al*., 2014. A scalable and efficient user authentication scheme for cloud computing environments. Proceedings of the 2014 IEEE International Symposium on Region 10, April 14-16, 2014, IEEE, Kuala Lumpur, Malaysia, ISBN:978-1-4799-2027-3, pp: 508-513.

Ramgovind, S., M.M. Eloff and E. Smith, 2010. The management of security in Cloud computing. Proceedings of the Information Security for South Africa, August 2-4, 2010, Sandton, Johannesburg, pp: 1-7.

Yang, G., D.S. Wong, H. Wang and X. Deng, 2008. Two-factor mutual authentication based on smart cards and passwords. J. Comput. Syst. Sci., 74: 1160-1172.

Yang, J.H., Y.F. Chang and C.C. Huang, 2013. A user authentication scheme on multi-server environments for cloud computing. Proceedings of the 2013 9th International Conference on Information, Communications and Signal Processing (ICICS), December 10-13, 2013, IEEE, Tainan, Taiwan, ISBN:978-1-4799-0434-1, pp: 1-4.

Zhang, M. and Y. Zhang, 2015. Certificateless anonymous user authentication protocol for cloud computing. Proceedings of the 2015 International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS), December 19-20, 2015, IEEE, Halong Bay, Vietnam, ISBN:978-1-5090-0464-5, pp: 200-203.