VOL. 10, NO. 23, DECEMBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

PRESERVING USER PRIVACY WITH ANONYMOUS AUTHENTICATION IN CLOUD COMPUTING

Mohd Izuan Mohd Saad, Kamarularifin Abd Jalil and Mazani Manaf
Faculty of Computer and Mathematical Sciences, UiTM Shah Alam, Selangor, Malaysia
E-Mail: mdizuansaad@gmail.com

ABSTRACT

Cloud computing offers its flexibility and dynamic nature in terms of its access to resources anytime and anywhere. All data and other resources in cloud storage are managed and controlled by the Cloud Service Provider. They provide security and ensure that the data is protected and free from any vulnerability. However, providing privacy through authentication mechanism is a big challenge. Most of the current authentication schemes rely on trusted third party to identify and verify user's credential which can lead to transparency issue. In order to ensure for a secured transaction, they have to preserve user's privacy from being exposed. The reveal information of user's credential will make it easier for attacker to gain the information for accessing to classified data. They can intercept and manipulate user's identity to gain access to sensitive data of user in the cloud storage. This issue can be solved by introducing anonymity features in the authentication scheme by hiding the user's information as well as to protect the user's identity from getting abused. Anonymity will protect user's identity by hiding the real users' identity during the authentication process especially when users have to deal with third party in their communication. The threat does not only come from external attacker but also comes from internal party who has full authority access to the server. This paper proposed an anonymous authentication scheme which is a combination of password-based authentication and anonymity feature in order to preserve user's privacy without involving the trusted third party during the authentication process. As a result, it can guarantee a secured transaction with anonymity features to protect user's privacy. This paper also presents the description of data privacy and security which can influence user's trust in using cloud services. Security analysis descriptions of possible attacks to the proposed scheme are also presented in this paper. The Secure Remote Password (SRP) protocol is used for this project with some enhancement to algorithm. In the future, the proposed scheme will be tested with some of the possible attack threats to prove that it is secured against the attack. The significant of this research is to preserve user's privacy with anonymous password-based authentication in the cloud environment without any requirement to trusted third party which can resist from vulnerability to attacks.

Keywords: privacy, anonymity, key exchange, password-based authentication.

INTRODUCTION

The growth of advanced technology in networking and related areas has required technical experts to restructure their existing infrastructure. Cloud computing is a new advanced technology which is composed of four deployment models, five essential characteristics and three service models [1]. With all the elements mentioned above, cloud computing has become the primary focus on government and business organizations such as IBM, Apple, Google, Amazon and others to develop and deploy their system application in order to provide a fast and reliable services to their clients. However, security is one of the crucial areas that need to be given prior attention especially in the process of authenticating the legitimate user within the cloud domain. The cloud service provider should preserve the user's privacy and provide data protection in the cloud storage from being attacked by the adversary. Most of the existing authentication schemes usually involved a third party to verify and monitor the transaction process between the cloud service provider and the users [2]. It could lead to issues of transparency, and may be biased in certain situations in which the user cannot measure and control the security level and privacy of their cloud domain.

The users trust their service providers based on their experience, professionalism, number of projects handled and personnel in-charge. However, the trust issue is one of the top risks in providing services in cloud environment [4]. Trust becomes a crucial element to guarantee a well-planned development of cloud environment, to provide protection and privacy control, to provide the security method and to ensure the right access to cloud data. In order to provide privacy of the user's credential, the system should provide strong authentication mechanism to protect the information as well as to verity the authorized user. Nevertheless, the task of providing privacy through a secure authentication mechanism is one big challenge. The system developer should understand the system and network architecture, party involved, user's access, location of storage / server, and potential hacking. This paper will further discuss details in providing strong authentication scheme to preserve user's privacy in cloud environment.

This paper is organized in the following sections. Problem Background Section presents the research problems and contributions of the research. Related Works Section presents literature study related research work. The Proposed Authentication Scheme Section presents the proposed solution in order to provide anonymity in password-based authentication. Security Analysis Section briefly describes the proofs of possible attack to the

proposed scheme. Finally, section for Conclusion draws the conclusion of the proposed scheme and future works.

PROBLEM BACKGROUND

Authentication and key exchange protocol arrangement are fundamental processes in establishing a secure communication. Password-based authentication is a basic authentication scheme and has generated growing attention in recent years on providing secure access to the system application. User's ID and password will be provided to the registered user to gain access to the system. The password will be stored in the server and managed by the data centre's owner (in cloud computing it is managed by cloud service provider). Many researches were conducted to improve the scheme by combining user's ID and password with new method such as two factor authentication, biometric, certificate, smart reader card and many others [4]. Nevertheless, the feasibility of these approaches required extra device, increase cost, involve complexity of deployment, need an expert consultation and open to malicious attack. None of these technologies is a magic bullet for security protection and they also carry risk and vulnerabilities. Therefore, password-based authentication scheme is still relevant and suitable to be used in a dynamic and big scale environment because of its simplicity and convenience features. User can just memorize the user's ID and password without any additional devices requirement to support the scheme. However, the strong method is needed in the password-based scheme to ensure that it is proofed from any attack (insider and outsider) either in a secure or insecure network.

Another challenge to provide strong authentication schemes in cloud environment is to ensure that user's credential is not being abused during authentication process. User's identity should be kept hidden by providing anonymity features to protect user's privacy against an insider or outsider hacker. To provide anonymity in authentication mechanism becomes a bigger issue nowadays. The cloud users were often exposed to disclose their identity because they have no method to control and monitor the information stored in cloud storage. They cannot rely on a secure channel because some of the cloud users were given access in different platform and domain which are less protected on their communication channel. The use of anonymity element can improve trustworthy of the system and will eventually convince the user to use that system [5]. The reliability and reputation of the system can be increased by these 'trust' and it also shows the accountability of the cloud service provider by providing the services. Combining password-based authentication with anonymity feature will lead to trust, reliable and secure cloud infrastructure.

Our contribution of this paper can be summarized as follow:

1. The proposed anonymous password-based authentication proves that it can preserve the user's privacy by hiding the user's credential. The combination of secure remote password (SRP) protocol and anonymity feature will enhance the trust level among the cloud users.
2. The trusted third party is not required during the authentication process. The user and server can be authenticated in a mutual authentication process. This measure will reduce communication overhead from server and communication cost on the third party.
3. The proposed scheme can resist vulnerable attack such as dictionary attacks, replay attack, Man-in-the-Middle attack and many others. The advantage of this scheme is that password will not be transmitted over the network and user's identity will be replaced by an anonymous identity before it was sent to the server.

RELATED WORKS

Numerous studies have been conducted in recent years on securing user data in cloud computing. Authentication and authorization become a key foundation in providing secure communication among the cloud users. Nevertheless, despite various solutions being recommended there were still loopholes in their studies that need to be filled in.

Authentication schemes

Authentication means proper verification and identification process of user's credential through username and password. Both processes are meant to ensure that the user is genuine. This process is to allow or grant the right to access the system and any resources in cloud domain. Strong authentication scheme is required to protect cloud resources from vulnerable attack and other security breaches. Authentication is the most important key issues among security issues of cloud computing [6]. Key establishment in the process of authentication is a fundamental procedure to enhance the level of security in network communication over an insecure platform. The user will exchange secret key over the network for verification during the authentication process.

There are many authentication schemes being introduced to achieve high level of secure communication between two or more parties such as password-based authentication, biometric authentication, smart card authentication and many others [6][7][8]. Password-based authentication scheme has been widely used over years. It has become a common method used for authentication because of its simplicity and is easy to be implemented.

In 1981, Lamport's work has first proposed the remote user authentication over insecure network by providing the password table in the server for storing the user's password [9]. However, Lamport's scheme has faced many problems in managing the password table and suffered from high hash overhead, necessity of counter resetting and increase the storage capacity. Moreover, they need more space to store a password table. This scheme can still be compromised if hacker manages to gain access to the password table which could lead to data leakage. It was also vulnerable to many attacks such as reply attack, dictionary attack, eavesdropping and Man in the Middle attack. Due to above reason, many researchers have

proposed a new method of remote user authentication by using smart card [8]. Smart-card authentication does not require the server to keep password table thus it can save more space in storage. However, this scheme requires additional device such as smart reader and it will incur cost for this device. There is also another issue if the smart-card is stolen, the attacker can impersonate the user to login the system illegally. Here are some of the issues related to the scheme:

1. They need expertise to setup and install additional devices such as a fingerprint scanner, which require extra cost and energy during installation and troubleshooting;
2. Dynamic and huge number of users will lead to constraints of performance and transaction time when all the users are being verified at the same time;
3. Some other devices such as mobile devices are not suitable with the current setting and need more work to reset and reconfigure;
4. Not all machines can support smart card reader and some other machines are not supported at all. It gets complicated when dealing with public terminal such as hotel or airport.

Diffie-Hellman protocol is a method that enables two users to share a secret key and agree to exchange the information over insecure network [10]. This method allows user's credential to be transmitted over the network which can cause attack such as Man-in-the-Middle attack. It can also compromise a user's privacy by exposing the user's credential without any protection. Password-Authenticated Key Exchange (PAKE) has been introduced by combining key exchange scheme and password-based authentication technique [11]. This scheme uses one-way function to generate verifier and all party involved to compute the secret key. However, this scheme suffers on protecting the verifier from malicious attacker and the corresponding secret password is still needed.

Many of the cloud service providers face significant security challenges and suffer the vulnerability of malicious attack including identity theft and data leakage [12]. There is a reason, why anonymity is needed in the architecture of cloud infrastructure. Slamanig's scheme has proposed the anonymous authentication by using public key which include verifiable and revocable anonymity [13]. Recently, there was arising issue on preventing secret key in mutual authentication which can lead to impersonate attack [14]. User faces difficulty to change the private key without a server or generator if they find out that their private key has been compromised and tend to be vulnerable by impersonate attack. Our proposed scheme use key generator to compute the private key. Each client and server will compute the private key on their own and will not be sent over the network. This will prevent the impersonate attack to our proposed scheme. In 2006, Das *et al*. proposed a dynamic ID-based remote user authentication scheme using smart cards [15]. However, this scheme is susceptible to various attacks which can lead to the security breach. This scheme also does not provide mutual authentication between user and server which can compromise the transparency of communication and is open to the man-in-the-middle attack. Table-1 shows the summary of functionality comparison between the proposed scheme and the related works.

Data privacy and security

Sharing and dynamic infrastructure is one of the cloud computing characteristics. All resources including database, system application, and backup data are stored in a shared environment. This situation is risky to the data since they can be disclosed and accessed by unauthorized user. It is truly a challenge to protect the user's privacy especially in a sharing environment. Privacy refers to protection of not only personal identity information but also to sensitive and confidential business information which can be accessed directly from cloud system application. The exposure of the user's privacy will also affect security process of the business operation [1]. Many organizations still do not have the trust and refuse to use cloud services not because of the total cost ownership but because of data privacy and security issues [16]. In the Cisco's CloudWatch 2012 [17] report shows that the security and privacy still remain the biggest barrier to wider adoption of cloud computing which is 54% respondents as compared to 2011 with 76% respondents.

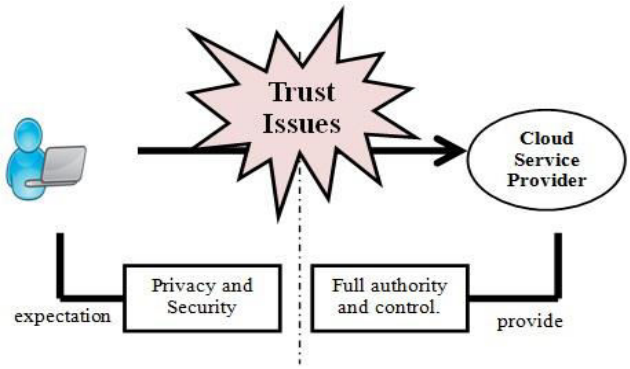

Figure-1. Overview of relationship of trust issues.

Figure-1 is an overview that shows user's expectation and what cloud service provider could provide in cloud services. In this case, cloud service provider has full control and manage the user's data without revealing and sharing the security method on how they protect the data. On the other hand, user expects transparency of security and privacy control by the cloud service provider. Unfortunately they did not get the full report of it. This gap will raise the trust issues when both parties do not get what they need and the other party does not allow and share what they provide. This is the main concern when the organization has decided to move their system to the cloud environment The mutual agreement between both parties has to be clear especially when negotiating with privacy and security issues. There are many choice of mechanisms for the user to ensure their data privacy such as Service Level Agreement (SLA) verification based reputation based, Cloud Trust Authority and many others [2].

Table-1. Functionality comparison of related schemes.

Description	Lamport [6]	Bellovin et al. [9]	Das et. al [15]	Our scheme
Session key agreement	Yes	Yes	Yes	Yes
Mutual authentication	No	No	No	Yes
Computation cost	Very Low	Low	Very Low	Very Low
User Anonymity	No	No	No	Yes
Non-dependency of third party	No	Yes	No	Yes

The decision to appoint trusted third party in authentication process risks an organization which could lead to security breach. Users will send their user's credential to the trusted third party for verification process before they can allow them to use the system. In some cases, cloud service provider is hired to be a trusted third party which could be bias for them to control and manage data privacy and security. This step is also vulnerable to insider and outsider attack because cloud service provider has full access including security control on the users' data. Users have to take the risk of assuming that the trusted third party will act as what they expected even though they do not receive any full report on security analysis. Users will lost control of their own data and have to rely the trusted third party to handle the security policies, user's access rules, monitoring and enforcement. The lack of trust among the cloud user by taking the risk of hiring the third party will make things worse. Thus it is important for user to know who created the data, who modified it and when the data is created. Provenance information (historical data) could be used to trace the data information, auditing and forensic activities. Due to this reason, data provenance and privacy element should be balanced together in clouds to achieve trust among the parties involved. System admin should look at this clearly in order to preserve the user's privacy in cloud environment.

SECURE REMOTE PASSWORD (SRP) PROTOCOL

Following the discussion above, it shows that password-based authentication is still relevant to be applied but it has to go through some modification and enhancement to ensure both security and privacy are protected. In this research, Secure Remote Password (SRP) protocol will be used to establish communication by using password-based authentication mechanism. Secure Remote Password (SRP) [18] is a password-based authentication protocol that provides zero-knowledge proof and it is a popular choice by the IETF for strong password protocols. This protocol uses an asymmetric algorithm to prove knowledge of a password without revealing the actual data. The SRP offers strong solution to secure the authentication process. It does not require any external or additional infrastructure/device and can be operated securely over insecure networks. This protocol can assure that:

1. It does not require password table in the server to store any information of password equivalents. In this protocol, the password will be computed together with random number known as salt number to generate the verifier value. Therefore, the attacker will not be able to guess or even if they can gain access to the server they still fail to predict or capture the real password. It also protects the server from dictionary attack;
2. Its verifier is values that replace the password for verification purpose during the login process. This is what they called as "verifier-based" which protect from password being stolen if there is any hacking or attack attempt. The server will use verifier value to prove knowledge of the legitimate user. Thus, the password is never sent via network. If the attackers get access to the server, they cannot use verifier value to authenticate because it requires both sides to verify the process which is called as mutual authentication process.
3. It provides strong session key establishment without revealing the key in public. Both user and server will establish a new session key every each login session. Thus, there is no useful to eavesdropper because the session key is different for each processing task.
4. Both parties have to verify each other before they can start to communicate. This is what they called "mutual authentication" by sending the evidence message for verification purposed. The advantage of mutual authentication is to allow the user to communicate with the server even in an insecure network.
5. It does not require trusted third party: It does not involve any third party for verification or identification of user credential. It can also avoid overhead that equivalent with PKI-based scheme [19].

The SRP has advantages from technical view and practical implementation. Therefore, it is suitable to be applied in a dynamic and flexible environment such as cloud computing. The advantages of SRP are as follows :

1. SRP is a simple and easy protocol to be implemented in system communication because it does not involve a complex mathematical calculation but simple exponentiation, addition, multiplication, and hashing, which are easily to be understood.
2. SRP has a low computation cost which can provide fast authentication process. It can operate as fast as conventional protocol such as Diffie-Hellman which can minimize user-visible delay.
3. SRP also provides the efficient debugging and is easy to be modified and implemented to any standard of application system. With a simple operation and crypto logic algorithm, this protocol enables user to perform the component functions and integrate the existing algorithm to suit with the client requirement.

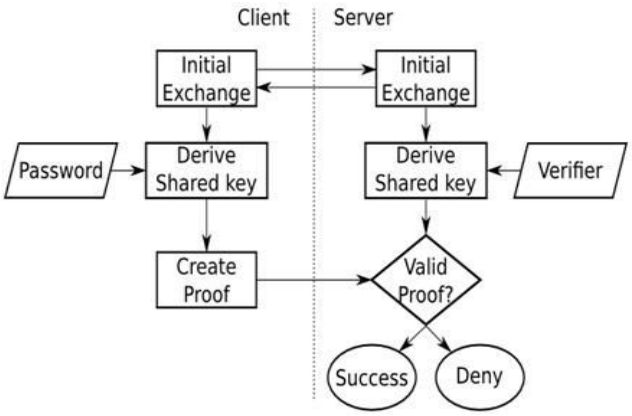

Figure-2. SRP workflow.

Figure-2 illustrates the workflow of the SRP process. The protocol uses its own SRP schema for key exchange that is based on username and password information. Initial exchange phase is a process of creating the verifier value and exchanging it between the user and server. The server computes the verifier value v for a user identity I and password P as follows [20] as equation (1) and (2):

$$x = H(s,I,P) \quad (1)$$

$$v=gx \quad (2)$$

Accordingly, the value v is stored securely together with random salt s in the server. Hence if an attacker obtains the verifier information stored on the server, they still fail to use this information as a client to authenticate it to the server. After establishing session key at both sides, client will generate message M1 and server generate message M2 for verification. This is what they called as authentication. The M2 is an optional for optimization of message order. It can reduce one step of handshaking process that will speed up the authentication time.

Aside from advantages of the SRP, there are some important issues that need to be considered. On the login phase, the user's name is sent to server as plain text. It is open to attacker to guess who is the user and its credential. Based on that information, the attacker can apply guessing attack to keep track the user password. Due to that reason, anonymity feature should be applied for hiding the user credentials and to prevent from various attack. Anonymous authentication can be applied by hashing the username with random salt number before it is transmitted over the network. Furthermore, the attacker can learn user's verifier that has been stored in server to masquerade as a real server. Another way is an attacker can also repeatedly do a trial and error to guess the user's password. In this case, introducing a time-stamp feature and set the limit on number of login attempt can reduce such attack

THE PROPOSED AUTHENTICATION SCHEME

In cloud computing, there are a few parties involved directly or indirectly to the system such as cloud user, data owner, cloud service provider and auditor. Each of these parties has their own role in the system. Communication in a dynamic, sharing and multi-party environment will expose user's identity information especially when they are communicating over insecure channel. Based on this reason, anonymity feature is one of the best solutions that can be applied in authentication process to secure and preserve user's privacy. Anonymous authentication recently becomes a hot topic for its use in hiding user's credential when user login into a system over a network. This mechanism can preserve user's privacy by applying anonymity feature into authentication process. Moreover, anonymization of identity information provides protection against identity theft and different types of linking attacks. In [12] has mentioned that in order to achieve a strong, reliable and secure system architecture, the system must be resilient to such attacks and have the capability to hide identities of communication participants from third parties.

In the SRP protocol, anonymous identity could be computed in the registration process. User will compute the anonymous identity (U) by hashing combination of user identity (I) and random salt number (s).

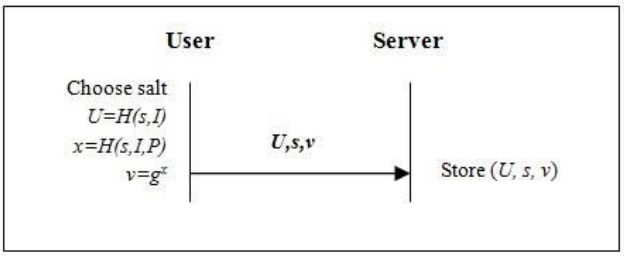

Figure-3. Registration phase

Figure-3 shows the registration phase which requires username and password from user to compute the anonymous identity (U) and verifier (v). Then, the three values (U, s, v) will be sent to server over the network. Based on this calculation, we stress that username (I) and password (p) will not be stored in the server or even sent over the network. A practical calculation to compute of U as equation (3) is as follows:

$$U = H(s,I) \quad (3)$$

After completing the registration, user can perform authentication with parameter identified. The handshaking process and establishing the session key (K) will be made by both parties for a mutual authentication procedure. By hiding the user's identity through this calculation, we could claim that the user's privacy is protected and the transaction is reliable throughout the anonymous authentication. This will give longer time for attacker to crack or hack the password because they have to find the identity of account first before they can proceed to the next step.

The advantages of the proposed scheme are as follows:
1. Prevent the leaking of user's identity or identity thief during the authentication process with anonymity feature.
2. Protect user's credential vulnerability to malicious attacks from an insecure and secure network.
3. Provide fast and efficient authentication time because of low computation cost.
4. Does not require additional devices or third party involvement during the negotiation session

SECURITY ANALYSIS

This section presents how the proposed scheme will provide the solution if they were be attacked. The proposed anonymous authentication scheme should be secured against any malicious attack. Here are some descriptions of proof for some possible attacks to this scheme:

1. **Dictionary attack** is trying to determine its decryption key or username/ password. It can divide into two scenarios; off-line attack and on-line attack. For off-line attack the attacker will suffer in trying all the possible random value of private key (a) and (b) which is not exposed publicly. For on-line attack, the attack will act as a user and will try to guess the username and password. The mechanism can limit the number of password attempt to block the attacker from trying constantly. Moreover, this mechanism uses a different session key for every login to authenticate with server.

2. **Impersonate attack** is an attacker trying to assume the legitimate user identity to perform an attack. It will not be able to impersonate the user if they don't have a session key (K). They cannot compute the evidence message (M1) and (M2) to prove that they are a legitimate user without having a session key (K). It becomes more complicated because the session key is not transferred over the network. User and server will compute their own session key (K) and will not share the key in public.

3**. Replay attack** is a form of network attack to the valid data transmission repeatedly. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). It cannot be done for this mechanism because the generation of key is randomness and it keeps changing for every login session.

4. **Man-in-the-middle attack** is when attacker secretly intercepts / tapping the communication between two parties and try to change and collect the information. It can only happen if the password and verifier are both known. Both values are required to conduct the attack. However, in this case it is difficult to get both values at the same time and it requires expensive work to do it.

5. **Stolen verifier attack** will happen if the attacker can gain access to the server and steal the user's verifier. It can impersonate as a legal server to manipulate the authentication process. However, this process cannot be done because it requires a user's password to continue.

6. **Anonymity protection** is to preserve user's privacy by replacing user's identity to be an anonymous identity. With an anonymous identity, not only attack from outsider but also insider cannot manipulate the value of identity. Anonymity value cannot be traced because it is a one-way hashing values which cannot be simply changed to its original value.

Table-2 shows the summary of the descriptions and proof of each possible attacks.

Table-2. Summary of security analysis.

Name	Description	Solution
Dictionary attack	- Attacker trying to determine its decryption key or username/ password - On-line or off-line attack	- Private key (a) and (b) are not exposed in public. - It's hard to attacker to guess the possible value of the key.
Impersonate Attack	- Attacker will try to assume the legitimate user identity to perform an attack.	- Session key (K) not sharing in public. - So, attacker cannot compute the evidence message (M1) and (M2) to prove that they are a legitimate user without having a session key (K)
Replay attack	- Attacker form of network attack to the valid data transmission repeatedly.	- Private key is random and it keeps changing for every login session.
Man-in-the-middle attack	- Attacker secretly intercepts / tapping the communication between two parties and try to change and collect the information.	- Can only achieve if both username and password are known which is impossible to do that.
Stolen verifier attack	- Attacker can gain access to the server as a legal server and steal the user's verifier.	- It requires a user's password to continue but the password are not stored in the server.
Name	**Description**	**Solution**
Anonymity protection	- Attacker try to stolen user identity to manipulate the info to get an access to the data.	- preserve user's privacy by replacing the user's identity to be an anonymous identity

CONCLUSIONS

The major obstacle of providing trustworthy in cloud services is a security issues. This paper has discussed related issues in order to preserve user's privacy and provide high level of security via authentication process. Authentication becomes a key issue among the security issues which should be given more concern. There are many researches carried out to ensure that the authentication of legitimate user is properly done in a secured process. The leaking of user's information and identity thief issues could lead to security breach. The intruder can manipulate the user's identity to illegally access the server or cloud storage. In this research, the Secure Remote Password (SRP) will be used to establish the authentication process with zero-knowledge proof. The SRP method has provided a strong solution to verify legitimate user without additional device or infrastructure requirement. It can also operate in an insecure network.

Anonymity is one of the elements that could hide the user's credential to preserve the privacy of user or organization. It can protect user's information from being abused by an attacker. It can also protect from being vulnerable to malicious attacks. Our proposed solution is to incorporate between the Secure Remote Password (SRP) schemes with anonymity features to become anonymous password-based authentication. This proposed scheme could provide high security level as well as preserve user's privacy in order to achieve high level of trust among the cloud domain.

Currently the work is in progress to formalize a more precise terms to prove its security features. The anonymous authentication scheme will be developed and performed for an experimental test to proof possible attacks as mentioned above. The finding and result of this experiment will be published soon.

ACKNOWLEDGEMENTS

The authors would like to thank Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM) for their financial support in funding this research.

REFERENCES

[1] Bowen J. A. 2011. Cloud computing: Issues in data privacy/security and commercial considerations. The Computer & Internet Lawyer, Vol. 28, No. 8, pp. 1-8.

[2] Huang J. and Nicol, D. M. 2013. Trust mechanisms for cloud computing. Journal of Cloud Computing, Vol. 2, No. 1, pp. 1-14.

[3] Ko R. K. L., Jagadpramana P., Mowbray M., Pearson, S., Kirchberg M., Liang Q. and Lee B. S. 2011. TrustCloud: A Framework for Accountability and Trust in Cloud Computing. 2011 IEEE World Congress on Services. pp. 584–588.

[4] Yassin A. A., Jin H., Ibrahim A., Qiang W. and Zou D. 2013. Cloud authentication based on anonymous one-time password. In Ubiquitous Information Technologies and Applications. pp. 423-431.

[5] Khattak Z. A., Manan J. A. and Sulaiman S. 2011. Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach. Journal of Advances in Information Technology. Vol. 2, No. 2, pp. 109–121.

[6] Jaidhar C. D. 2013. Enhanced mutual authentication scheme for cloud architecture. In Advance Computing Conference (IACC), 2013 IEEE 3rd International. pp. 70-75.

[7] Hasan R. and Khan R. 2014. Interaction provenance model for unified authentication factors in service oriented computing. In Proceedings of the 4th ACM conference on Data and application security and privacy. pp. 127-130.

[8] Mun J., Jin Q., Jeon W. and Won D. 2013. An Improvement of Secure Remote User Authentication Scheme Using Smart Cards. In International Conference on IT Convergence and Security (ICITCS). pp. 1-4.

[9] Lamport L. 1981. Password authentication with insecure communication. Communications of the ACM. Vol. 24, No. 11, pp. 770-772.

[10] Rescorla E. 1999. Diffie-Hellman key agreement method.

[11] Bellovin S. M. and Merritt M. 1992. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In Research in Security and Privacy. pp. 72-84.

[12] Khalid U., Ghafoor A., Irum M. and Shibli M. A. 2013. Cloud based secure and privacy enhanced authentication & authorization protocol. Procedia Computer Science. Vol. 22, pp. 680-688.

[13] Slamanig D. 2011. Anonymous authentication from public-key encryption revisited. In Communications and Multimedia Security. pp. 247-249.

[14] Mishra R. 2014. Anonymous Remote User Authentication and Key Agreement for Cloud Computing. Vol. 258, pp. 899–913.

[15] Das M. L., Saxena A. and Gulati V. P. 2004. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics. Vol. 50, No. 2, pp. 629-631.

[16] Kshetri N. 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy. Vol. 37, No. 4, pp. 372-386.

[17] Cisco CloudWatch Report 2012. Summer 2012. Retrieved from Website: http://www.cisco.com/cisco/web/UK/assets/cisco_cloudwatch_2012_2606.pdf

[18] Thomas Wu. 1998. The Secure Remote Password Protocol. Proceedings of the Symposium on Network and Distributed Systems Security NDSS 98. Pp. 97–111. Retrieved from ftp://srp.stanford.edu/pub/srp/srp.ps.

[19] Sajjad A., Rajarajan M., Zisman A. and Dimitrakos, T. 2015. A scalable and dynamic application-level secure communication framework for inter-cloud services. Future Generation Computer Systems. Vol. 48, pp. 19–27.

[20] Thomas Wu. 2002. Srp-6: Improvements and refinements to the secure remote password protocol.