International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Novel Authentication Technique in Cloud Computing

Prajakta Gajanan Mhatre
Student, Neral, India

***Abstract*: Cloud computing is an internet-based computing technology, where shared resources such as software, platform, storage, web services, and other information are provided to clients on demand. It is a computing platform for distributing resources that include infrastructures, software, applications, business processes, and web services. Cloud provides a virtual storage of computing resources that provide computing functions for users with the help of internet. Examples are Google Docs or Google Apps, YouTube, or Picasa Image sharing, Amazon's EC2, and many more. In this work, we propose an innovative authentication scheme for cloud computing, called as Message Digest Authentication (MDA) along with smart card generator (SCG) service and cloud computing service providers to achieve the strongest authentication of all. The performance of the proposed system is evaluated via protocol simulation, efficiency analysis, and security analysis. The proposed scheme provides security and comfort for mobile clients to access various mobile cloud computing services from numerous service providers using just a single key, which is nothing but a secret key. The proposed scheme is based on the concept of dynamic nonce generation and bilinear pairing cryptosystem.**

***Keywords*: Cloud computing, authentication technique, smart card generator, dynamic nonce generation, bilinear pairing cryptosystem.**

1. Introduction

Authentication is always referred to as the use of biometrics to guarantee that the resource is utilized by the same user throughout the usage span. Traditionally, cloud computing users can encrypt data before it is sent over cloud and then store it in the cloud to avoid security issues, but this is not true for mobile users, as encryption technique does not approve mobile devices due to the encryption process, which requires high workload and high CPU processing. As we know that mobile devices do not have enough computational power and the battery life, it is preferable to perform much of the resource-intensive tasks at the cloud server. The mobile device can only be used as a channel for transferring data over cloud or as a viewer for visualizing the final result. The primary security concern in cloud computing is securing remote data and applications from unauthorized access. There is countless security issues associated with cloud computing, but most prominently these issues fall under two broad categories:

- Security issues faced by cloud service providers such as, businesses providing software-as-a-platform or infrastructure-as-a-service through the cloud, for example, Amazon, Google etc.
- Security issues faced by their clients (businesses, organizations, or individuals who host applications/ services or store their valuable data on the on the cloud).

While authenticated users can access their cloud data, the cloud provider can also do so and is called as privacy issue. Privacy issues arise as the cloud model gives cloud service providers greater ease to control and thus, it can monitor all communication between the host company and the end user, and access user data (with or without permission). Many organizations, these days, use cloud computing services either directly or indirectly. For example, using services provided by Amazon or Google means we are directly storing data into the cloud. While Twitter is an example of storing data indirectly, as Twitter stores tweets onto the cloud. Data integrity should also be considered when talking about data authentication as it is nothing but completeness of data. Maintaining integrity of data in cloud computing means whatever is stored on the cloud should be consistent, but there is always the possibility that third parties such as, hackers will illegally access your cloud data and compromise your data which is termed as data integrity issue. Therefore, the security, privacy, and data integrity issues in cloud computing becomes one of the primary research area. Mobile users normally access various cloud computing ser- vices from a numerous service providers and it is a nightmare for users to sign up for different user accounts on each service provider and remember corresponding private keys or passwords for authentication. In this scenario, mobile users will definitely be interested in how to access different services from mobile cloud service providers by using the only one password or just one private key. To address these issues, we need to improve the mechanism of protecting access to the mobile cloud which in turn will improve the security overall, which, at least, protects the mobile cloud from illegal access. To overcome all these issues in cloud computing, we have proposed a novel authentication technique for mobile cloud computing called as Message Digest Authentication (MDA) along with smart card generator (SCG) service and cloud computing service providers to achieve the strongest authentication of all. The web browser or the cloud service application will mutually authenticate both the cloud service provider and the

user. After authentication, the user can access the resources and available services from the cloud service provider. The proposed scheme provides security and comfort for mobile clients to access various mobile cloud computing services from numerous service providers using just a single key, which is nothing but a secret key. The proposed scheme is based on the concept of dynamic nonce generation and bilinear pairing cryptosystem. The scheme implements shared key exchange, mutual authentication, user anonymousness, and user un-traceability.

2. Review literature

While going ahead with the flow, it is important to gain a sight about issues relates to cloud computing authentication in general, and mobile cloud computing in specific. Accordingly, the literature work has been split into two parts as follows.

A. Cloud computing security

In year 2010, K. Popovic and v. Hocenski in [10] has discussed a number of security issues related to cloud computing. Their study shades some light on the remote location of resources and virtualization technologies that make the cloud computing environment vulnerable to attacks. All clients access a common resource location, which reduces the security. Furthermore, there is a data integrity issue in case of transfer, storage, and retrieval of user data. In year 2011, E. Mathisen [8] explains different cloud related policy issues. It is very difficult to trust any employee and the same is applicable to the cloud hosting company. If these employees are careless and un-trustable then, very positively, there is an ingrained vulnerability in the applications/service offered by them. In year 2012, Yandong ET [14] explains different types of clouds such as, public, private, and hybrid, and also the security- and safety-related issues associated with the public cloud. Public cloud is accessed by a majority of the general population without much restriction. Monitoring and standardizing administrator privileges is required for better authentication, security, and privacy. In year 2010, P. Urien, E. Marie, and C. Kiennert [13] have discussed a number of security issues related to cloud computing. This study is concerned about server administration in a secure system for both the service providers and its clients. This research affirms to solve this issue by proposing a solution based on a grid of smart cards built on a context of SSL smart cards. We trust that EAP-TLS server smart cards provide the security and the ease of use needed for administrating servers. Hence, we build the RADIUS server in a way that EAP messages are fully functioned by SSL smart cards. We also talk about the scalability of the RADIUS server linked to smart card grids. The computation in the server is managed by the mutual occurrence of numerous authenticating sessions. Lastly, we relate the results of the first experiment with the RADIUS server and an array consists of 32 Java cards, and briefly describe the feasibility and related scalability of this architecture.

B. Mobile cloud computing security

Increased use of mobile devices has promoted extensive research in the area of security in mobile cloud computing, and that to, majorly, on authentication as explained below. In year 2012, K.Y. Yoo [12] focuses on a cellular automata (GA) based lightweight technique, used for multiuser authentication in the cloud environment. The authentication is performed using a one- time password (OTP). Even though OTP-based authentication approach is considered to be secure, encryption is missing in this scheme as, Seed A is sent from the authentication server to user A without encryption. In year 2011, A. G. Revar and M. D. Bhavsar [11] describes the adequacy of single sign-on in a mobile cloud computing environment. Single sign-on (SSO) lays on the top layer of the cloud. Their research verified the single sign-on authentication scheme on an Ubuntu server. This scheme does not exactly addresses how a mobile device or any cloud-compatible device will access the cloud using SSO. In year 2011, Z. Ahmad, K.E. Mayes, S. Dong, and K. Markantonakis [1] proposed a security framework. The client authentication is done at boot time, and is dependent on USIM (universal subscriber identity module) response to a random challenge practiced by the cloud authentication service. This method works only for the mobile devices that support USIM and that is a major drawback in case, cloud users want to switch to mobile devices that do not make use of USIM, for example, tablets or laptop computers. In year 2009, W. Itani, Kayssi, and A. Chehab [6] proposed Privacy as a Service (PaaS); a set of security protocols for maintaining the privacy and legitimacy of the customer's data on cloud. The security solution is built on secure cryptographic coprocessors for acquiring a trusted and an isolated execution environment in the cloud. This paper also highlights the privacy enforcement mechanisms supported by PaaS protocols and the proof-of-concept implementation of the privacy protocols.

C. Analysis of the literature review

From the literature review section, we can list out few advantages and disadvantages in the existing system. They are listed below:

- Software used in authenticating a user in cloud comput- ing is vulnerable to external as well as internal attacks. So, by avoiding the use of only open source software in the system, the vulnerability can be reduced.
- Single sign-on (SSO) and one-time password (OTP) authentication systems are easy to implement, but in OTP data is sent from the authentication server to the user without encryption, which makes the system more vulnerable to external attacks.
- USIM-based authentication works only for mobile de-vices that support USIM, but what if a user wants to switch to other electronic devices that are not built using USIM? System might fail, in this case.

In cloud computing, there is absence of a common standard to ensure data integrity. Different vendors follow different structures for data storage and access, as a result of which switching vendors is not easy. Also, there is a need for common standard of encryption and decryption and client's control. Without proper encryption and security, transferring or storing user's confidential data is not possible.

3. Proposed system

Our proposed authentication system is purely based on bilinear pairing cryptosystem and dynamic nonce generation. It does not require any additional verification tables for the SCG service and cloud computing service providers.

A. Problem definition

Authentication is the process of verifying and validating the identity of an individual. Data stored on a cloud can be accessed by someone who is not authorized to do so. Since user's data is stored in unencrypted format to the remote servers, owned, operated, and maintained by the third-party cloud service providers, the risks of unauthorized access of the user's confidential data is very high. Therefore, security is a major and vital concern in cloud computing environment, as it may cause a potential damage to privacy and confidentiality of data, if user information or transmitted data are compromised. Hence, it is necessary to address security, privacy, and data integrity issues in mobile cloud computing during authentication. Authentication is commonly done through the use of pass- word and pin, using finger print (biometric), using SMS, digital signatures, secure socket layer, Kerberos, and many more ways, but these techniques are not efficient enough to protect user's identity over a cloud as each technique has its pros and cons.

B. Proposed technique

From above all discussed points, it makes sense to design an authentication system, which can provide strong authen- tication and still is easy to implement. With MDA, smart card generator (SCG) service, and cloud computing service providers, the system uses identity-based cryptography in the proposed project. Identity-based cryptography is the second form of the Public Key Cryptography in which a publicly available string representing an individual or organization is used as a public key. The public string could be consists of an email address, a domain name, or an IP address. The first implementation of identity-based signatures and an email based public-key infrastructure (PKI) was implemented by Adi Shamir in 1984 and that allowed users to validate digital signatures using just the public information such as user's identity. As per Shamir's scheme, a trusted third party would deliver the private key to the user only after his authenticity is verified and essentially, it should be the same as that required for issuing a certificate in a typical PKI. Security analysis for the proposed scheme is carried out here to show that the proposed scheme achieves user-to-service provider authentication, service-provider-to-user authentication, and the key agreement under random oracle in theorems respectively. The SCG is accountable for generating and broadcasting the private keys to the users and service providers safely. If a service provider or a user joins the system, the SCG is not required to update its master key or corresponding public key. When a user obtains his/her private key, he/she can authenticate and communicate with the other authentic entity by using his/her private key without the help of the SCG.

C. Proposed system architecture

This paper describes the scheme for authentication that is consist of three phases i.e., system setup, registration, and authentication. Let us explain each on by one

1) System setup phase:

- First, SCG generates any random number as its master private key.
- Then, SCG computes the corresponding public key, and generates all public parameters.
- Finally, the SCG publishes its public key and public parameters.

2) The registration phase:

- First, the mobile user and service providers are required to register with the SCG by sending their identities.
- Upon receiving these identities, the SCG computes and generates corresponding private keys for these users and service providers before dispatching these keys back to corresponding users and service providers securely.
- In accordance with the design of identity-based crypto system, the identities of the mobile users and service providers are also served as their corresponding public keys. Fig. 1 shows the flow diagram of registration phase.

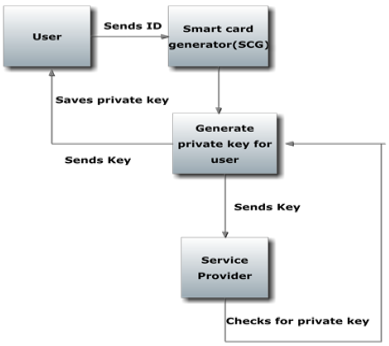

Fig. 1. The flow diagram of the registration phase

3) The authentication phase

- The mobile user and the targeted service provider authenticate each other without the involvement of the SCG.
- A session key is also generated during authentication to encrypt/decrypt subsequent messages sent between the user and the service provider after authentication.

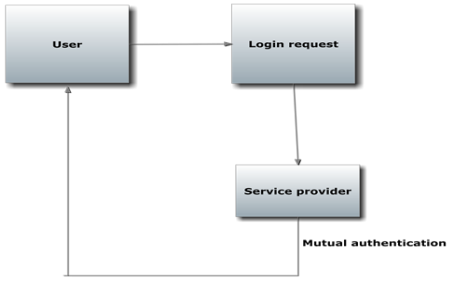

Fig. 2. Shows the flow diagram of authentication phase

D. Advantages

The proposed system has the following advantages

- The proposed method reduces the usage of memory spaces on the respective service providers.
- This technique makes sure both parties are having secure and efficient way of communication over a cloud. It reduces the overall authentication processing time required for communication and computation between cloud service providers and the trusted third-party services. Fig. 4 shows the flow diagram of the proposed system and Fig. 3 shows the entire architecture framework of the proposed authentication scheme.

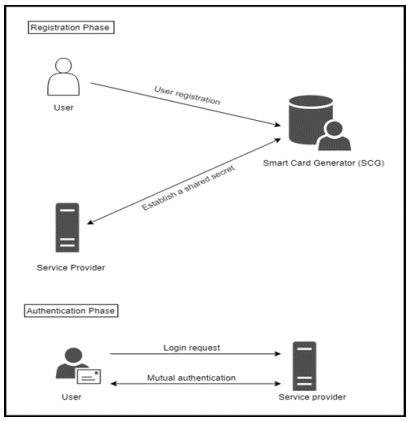

Fig. 3. Architectural framework of the proposed authentication scheme

E. Modules

The proposed authentication scheme has total four modules:

- Registration module
- Authentication module
- SCG module
- Service providing module

Each module is described one by one.

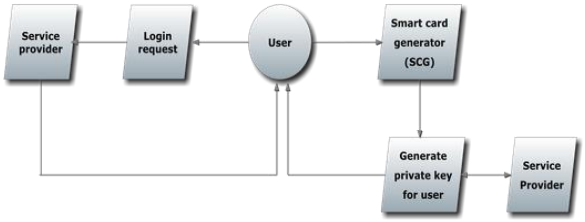

Fig. 4. The flow diagram of the proposed system

1) Registration module

In this module, the users who want to use the cloud services should be registered first. For that the scheme provides mutual authentication, key exchange, user anonymity, and user un-traceability. When a user wants to sign in with the Smart Card Generator (SCG), the user first provides his/her credentials. Fig. 5, shows the diagrammatic representation of registration module.

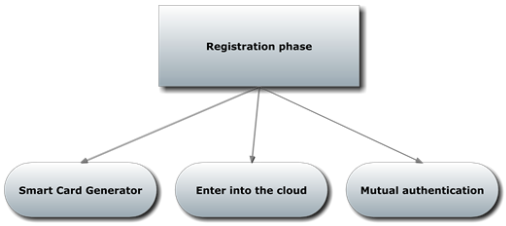

Fig. 5. Registration module

2) Authentication module

When a user wants to sign in with the service provider, he/she first provides his/her password. The password is randomly generated by SCG using a key generator. After that SCG validates the password and authenticates the user to access the service provider as shown in Fig. 6.

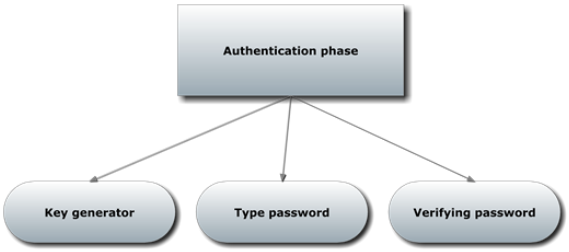

Fig. 6. Authentication module

3) SSG module

In this module, when a user wants to communicate with the service provider, the user first credits his/her password. SCG is responsible for generating and distributing the private keys to the users and service providers, respectively. If a cloud service provider or a user joins the system, SCG is not required to update its primary key or a relative public key. After obtaining his/her private key, he/she can authenticate and communicate with the other legit entities using his/her private key instead of using SCG as shown in Fig. 7.

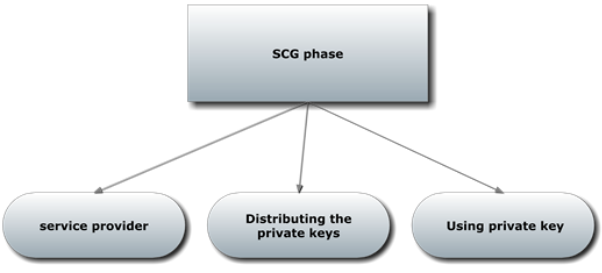

Fig. 7. SSG Module

4) Service Providing Module:

When a user wants to log in with the service provider, the user provides his/her password. Then the third-party service provider offers services to the users. The single user can access multiple service providers using the same private key generated by SCG for user anonymity, mutual authentication, and the key exchange as shown in Fig. 8.

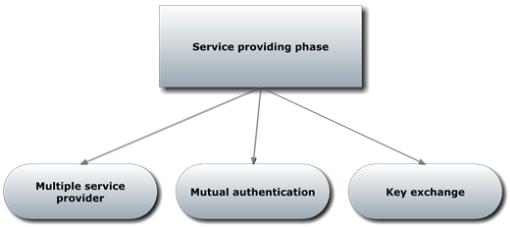

Fig. 8. Service providing module

F. Proposed algorithms

Following is the proposed algorithm

1) Collision Attack Algorithm

The collision attack algorithm, as far as cryptography is concerned, tries to find out two inputs that produce the same output on a cryptographic hash, also called as a hash collision. This is in contrast to a pre-image attack where the hash value is not specified. There are broadly two types of collision attacks, as follows:

2) Collision attack:

- This type of attack looks for two different messages m1 and m2 such that their hash will match, that is, hash(m1) = hash(m2).
- Chosen-prefix collision attack: In this attack, if two different prefixes p1, p2 are given, the algorithm searches two appendages m1 and m2 such that h

In a traditional collision attack, the intruder cannot control what content of a message to be attacked, rather the content is arbitrarily selected by the algorithm. As symmetric-key ciphers are very much prone to a brute force attack, every cryptographic hash function is essentially prone to collisions using a birthday attack. Because of the birthday problem, these attacks are much quicker and faster compared to a brute force attack. Therefore, we can consider breaking a hash of n bits into 2n/2 time (evaluations of the hash function). This way collision attack can be made faster than the birthday attack and the obtained has function is termed as "broken". If we want more efficient attacks to be implemented then it's possible by practicing cryptanalysis of the specific hash functions. The NIST hash function competition succeeded in persuading that the published collision attacks generally happen against two often used hash functions, MD5 and SHA-1. Even though, the collision attacks against MD5 have improved so much that it takes just a few seconds to execute on a regular system, hash collisions produced using this way are usually of the constant length and mostly unstructured, so cannot directly be used to attack large protocols. However, workarounds are possible for example, use of abusing dynamic constructs present in the many formats. In this method, two documents would be created which will resemble to each other so that to produce the same hash value out of it. One document would be presented to the CA authority to be signed, and then that digital signature could be copied and pasted to the other file. This kind of document would contain two different types of messages in the same document, but might display one or the other through mild changes to the file:

- There are a few document formats like PostScript, or macros in Microsoft Word that have conditional constructs for example, if-then-else that help in testing of the documents and identifying whether the location in the file has one value or the other in order to control what is visible.
- TIFF files can contain cropped images and display a different part of an image every time it is accessed, but without affecting the hash value.
- PDF files are more vulnerable to collision attacks by using a color value, such that the text in one message is displayed in white color and it blends into the background, while the text in the other message is displayed in some dark color, which can then be altered or tampered to change the content of the digitally signed document.

We also have an extension of the collision attack called as, the chosen-prefix collision attack, which is specific to Merkle Damgard hash functions. In this attack, the attacker can choose two randomly different documents, and then append different calculated values that result in the all the documents having an equal hash value. This attack is much more powerful than a classical collision attack. Mathematically stated, given two different prefixes p1, p2, the attack finds two appendages m1 and m2 such that hash(p1 m1) = hash(p2 m2) (where is the concatenation operation).

Message Digest Algorithm: In the proposed scheme, a mobile device has to be registered with a cloud server as a prerequisite process prior to avail any kinds of cloud services. The data transmission between the mobile device and the cloud server must be performed once the mobile device authenticates the cloud server and vice-versa. A strong authentication scheme ensures secure communication between two legitimate parties even if the communication channel experiences potential vulnerability and for that we are using MDA. MDA is a one-way cryptographic function that accepts an entity of any length as input and returns a fixed-length encrypted value to be used for authenticating the original entity. It is indeed that it is mathematically impracticable to generate two entities having the same message digest, or to produce anything having a given pre-specified target message digest. MDA is intended for digital signature applications, where a large file must be compressed in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA:

Take the input and append padding bits to the tail of the message.

Table 1
Comparisons with other existing schemes in terms of security properties

	[3]	[5]	[9]	[2]	[4]	[7]	Ours
Reluctance to replay attack	×	×	C	C	C	C	C
Providing user anonymity	×	×	×	×	C	×	C
Providing user untracability	×	×	×	×	×	×	C
Reluctance to offline password attack	C	C	C	×	C	C	C
Reluctance to time synchronization problem	×	×	×	×	C	C	C
Reluctance to forgery attack	×	×	×	×	C	C	C
Favorability to multiple service providers environment	×	×	×	×	×	C	C
Security proof	×	×	×	×	C	×	×

- Then append length to the previously generated message.
- After that initialize the MD buffer.
- Process the message.
- Output the secret message aka the message digest.

4. Results

In this section, numerous experiments are conducted to analyze the security of proposed system. In order to evaluate security strength of a proposed authentication scheme, security analysis based on formal proof technique is conducted.

A. Security analysis

This section compares the proposed authentication scheme with existing authentication schemes [3] [5] [9] [2] [4] [7] in terms of security. From the Table 1, it is clear that only our scheme and the scheme proposed in [4] have conducted formal proof process in terms of security strength. Existing schemes introduced in [3] and [5] [9] [2] are also vulnerable to several security threats. For example, the schemes in [3] and [5] are vulnerable to replay attack, time synchronization problem, and forgery attack; the existing scheme in [9] is vulnerable to time synchronization problem and forgery attack; and the scheme in [2] is vulnerable to offline password guessing attack and forgery attack.

B. Efficiency analysis

In this section, we will compute the performance efficiency in terms of computation time, as shown in Table 2 and Fig. 9.

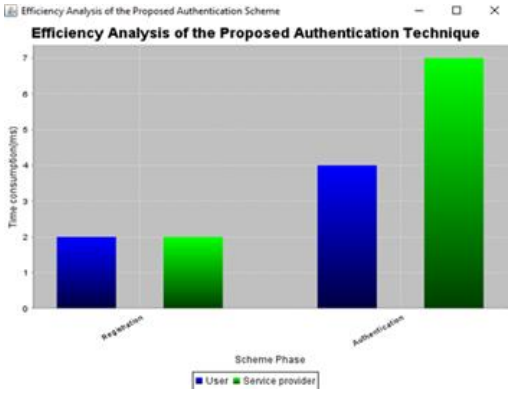

Fig. 9. Efficiency analysis of the proposed scheme in real time

Table 2
Efficiency analysis of the proposed scheme

Scheme Phase	Party	Time Consumption
Registration	User	Tm
	Service Provider	Tm
Authentication	User	3Tm
	Service Provider	2Tb+4Tm

5. Conclusion

As per our research the proposed novel authentication system makes use of a smart card generator service and the cloud service providers to secure user's identity. This system proposed a new authentication scheme for mobile cloud services environment. This scheme is very efficient and secure too. The system used Smart card generator to generate keys in this project. This system allows a mobile user to access multiple services from different mobile cloud service providers using only one single private key. The proposed scheme supports mutual authentication, key exchange, user anonymity, and user intractability. Security analysis have shown that the proposed authentication scheme withstands all major security threats and meets general security requirements. The system does not needed any verification table to be implemented at service providers or the trusted SCG service. The trusted SCG service is not involved in individual user authentication process in this proposed system. With Smart card generator, the system reduces authentication processing time required by communication and computation between cloud service providers and traditional trusted third party service. As security strength of the proposed scheme is based on nonce and bilinear pairing, the scheme itself is not subject to time synchronization problem and can be easily implemented in mobile cloud computing environment.

6. Future Scope

Cloud authentication and cloud security challenges are a part of never ending research. The following are the various issues that need to be identified as a future scope:

- *Data categorization using authentication:* A cloud can store data from vast number of users. In order to provide the top notch level of security to them for the value of data, categorization of data can be done. This categorization scheme should take into account different aspects like data category, its frequency, and access by various stakeholders. Once the data is sorted

and tagged, then the level of security concerned with this particularly tagged data can be provided.

- *Secure and trust based system for cloud computing:* A secure box for executing the cloud services by also taking into consideration the overall security constraint is a challenge. An authentic, secure, and trustworthy solution is the need that needs to be addressed by the cloud infrastructure.
- *Optimal use of resources:* While focusing on the security aspect of the computing, the optimum use of cloud infrastructure also needs to be considered.

References

[1] Z. Ahmad, K. E. Mayes, S. Dong, and K. Markantonakis. Considerations for mobile authentication in the cloud information security technical report, 16(3-4):123–130, 2011.

[2] T.-H. Chen, H.-l. Yeh, and W.-K. Shih. An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. In Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on, pages 155–159. IEEE, 2011.

[3] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak. A novel remote user authentication scheme using bilinear pairings. Computers & Security, 25(3):184–189, 2006.

[4] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak. A novel remote user authentication scheme using bilinear pairings. Computers & Security, 25(3):184–189, 2006.

[5] T. Goriparthi, M. L. Das, and A. Saxena. An improved bilinear pairing based remote user authentication scheme. Computer Standards & Interfaces, 31(1):181–185, 2009.

[6] W. Itani, A. Kayssi, and A. Chehab. Privacy as a service: Privacy- aware data storage and processing in cloud computing architectures. In Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on, pages 711–716. IEEE, 2009.

[7] H. Li, Y. Dai, L. Tian, and H. Yang. Identity-based authentication for cloud computing. In IEEE International Conference on Cloud Computing, pages 157–166. Springer, 2009.

[8] E. Mathisen. Security challenges and solutions in cloud computing. In Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, pages 208–212. IEEE, 2011.

[9] A.-S. K. Pathan and C. S. Hong. Bilinear-pairing-based remote user authentication schemes using smart cards. In Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, pages 356–361. ACM, 2009.

[10] K. Popovic´ and Ž. Hocenski. Cloud computing security issues and challenges. In MIPRO, 2010 proceedings of the 33rd international convention, pages 344–349. IEEE, 2010.

[11] A. G. Revar and M. D. Bhavsar. Securing user authentication using single sign-on in cloud computing. In Engineering (NUiCONE), 2011 Nirma University International Conference on, pages 1–4. IEEE, 2011.

[12] S.-H. Shin, D.-H. Kim, and K.-Y. Yoo. A lightweight multi-user authentication scheme based on cellular automata in cloud environment. In Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on, pages 176–178. IEEE, 2012.

[13] P. Urien, E. Marie, and C. Kiennert. An innovative solution for cloud computing authentication: Grids of eap-tls smart cards. In Digital Telecommunications (ICDT), 2010 Fifth International Conference on, pages 22–27. IEEE, 2010.

[14] Z. Yandong and Z. Yongsheng. Cloud computing and cloud security challenges. In Information Technology in Medicine and Education (ITME), 2012 International Symposium on, volume 2, pages 1084–1088. IEEE, 2012.