International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Security as a Service by Verification using Information System (Info-Sys) in Cloud Network

Debabrata Sarddar, Sougata Chakraborty

Abstract: ***Security in Cloud Network is essential and data security is required when data is transmitted from the sender device to receiver end and vice versa. Sometimes, the eavesdroppers might steal sensitive data which is dangerous for the users of the cloud network. The goal of the paper is to propose a newer dimension to Cloud Computing - 'Security as a Service by verification using Information System in Cloud Network' in which an authentication procedure is used from the user side to ensure the privacy of the network. AES algorithm is used to encrypt the Unique Identification Number (UID) provided by the user to hide from the eavesdroppers and decrypt the same at the receiver end. In this algorithm, the same key is used for encryption and decryption process. Therefore, the sender and the receiver must know and use the same secret key. We have introduced an Information System that keeps track of all users and helps during the verification. Decryption of the encrypted UID will also be done in this system. It also helps to manage session of all users who have logged into the system and tries to access the information with the UID. If the user shares one's UID with other personnel and if it causes any problem of insecurity in organizational network, then it will also be caught by the Information System. This helps to protect the cloud network from the trespassers and increases security of the network.***

Keywords: AES, data security, Information System, Security as a Service by verification, network security, unique identification number.

I. INTRODUCTION

Cloud computing security mainly deals with the network security and the data security or the information security. It is implemented to protect the data, application and other infrastructure of the cloud network. Cloud service providers and their customers face the problem of security issue in the cloud. Data security and application protection should be ensured by the service provider. The user should also provide strong password, unique and secure code for authentication to enhance the security of his/ her own as well as the cloud network.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Debabrata Sarddar*, Assistant Professor, Department of Computer Science and Engineering, University of Kalyani, West Bengal, India.
Sougata Chakraborty, Senior System Engineer, IBM India Private Limited in Kolkata, India.

In public cloud, there is a probability of information access by other users of the network which hampers the security of the information. The network may face the problem of insider attack. For this reason, the service providers must check the users who all are available in the data centers of the network and any kind of suspicious activity is notified to the user [3].

II. SECURITY AND PRIVACY IN CLOUD NETWORK

A. Identity management

Biometric-based identity management will be the best identity management procedure of the customer. Users can also manage their identity of their own. Cloud ID is an identity management tool.

B. Physical security

Cloud service providers physically secure the hardware from unauthorized access, theft and natural disasters.

C. Personnel security

The information security is associated with cloud services that are typically handled through security screening potential recruits, security awareness and training programs.

D. Privacy of the Cloud Network

Authorized users have access to data to the cloud network. Digital Signature, strong password and application of encryption algorithm over sensitive and confidential information can increase the privacy of the network.

III. SECURITY OF CLOUD NETWORK

There are many security threats in cloud data services such as network eavesdropping, illegal invasion, and denial of service attacks, side channel attacks etc. Security parameters of cloud data are discussed below:

A. Confidentiality

It means that data contents are not open to unauthorized users. Only authorized users can access the sensitive data of the network. Data owners look forward to exploit cloud data services without the any leakage of the data contents [1].

B. Access Control

Data Access Control deals with the restriction of access to user data stored in the cloud network. Some legal users can be authorized by the owner to access the data, while any other trespassers are not allowed to have whole access over the data [1].

C. Integrity

Data integrity maintains and assures the accuracy and completeness of user data. A data owner always thinks that his/her data in a cloud network is stored correctly.

IV. OVERVIEW OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

The AES algorithm is an encryption algorithm [18], [19], [20] that uses symmetric key. The encryption technique is used to convert the plaintext to its equivalent ciphertext and decryption technique is used to convert the ciphertext to its equivalent plaintext form. The AES algorithm can encrypt and decrypt the data of 128 bits in size. The length of the key used for this algorithm can be 128, 192, 256 bits in size at different rounds respectively.

Fig.1 shows the schematic structure of Advanced Encryption Standard algorithm that suitably explains different rounds to obtain cipher text from plain text.

Fig. 2 shows the encryption process.

Byte substitution - Byte substitution is done by the S-box design. This is a matrix of four rows and four columns.

Shift Rows - Each row is being shifted towards left. Each entry in decreasing order is re-introduced on the right-hand side of the row.

Mix Column - The 4 bytes of a single column is taken as input and the output produced is completely new 4 bytes. The output replaces the original column.

Add round key - The XOR operation is done between the 16 bytes of the matrix and the 16 bytes of the round key. The obtained output is a ciphertext in the last round. Otherwise, the process continues with the resulting 16 bytes to start the similar round.

The decryption process includes all the above steps but in reverse manner. Following two Figures show the whole schematic structure and the encryption process of AES respectively.

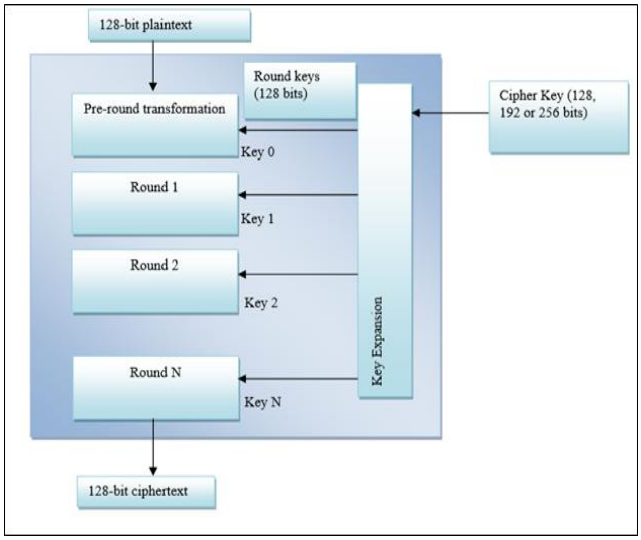

Fig. 1.Schematic structure of Advanced Encryption Standard

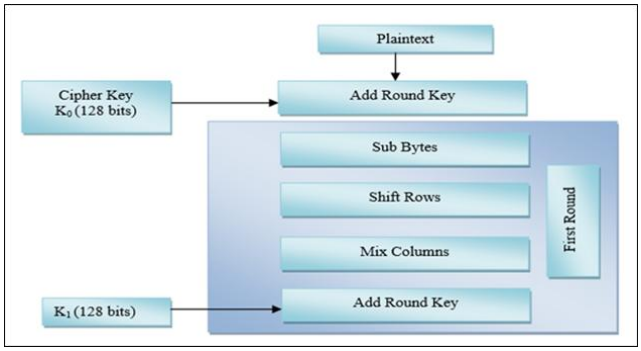

Fig. 2.Encryption process of AES algorithm

AES is used because it has several advantages over other cryptographic algorithms.

A comparative study over DES, AES, and RSA is illustrated below:

Table- I: Comparison among DES, AES and RSA at a glance

DES	AES	RSA
Symmetric Key algorithm.	Symmetric Key algorithm.	Asymmetric key algorithm.
Key size is 56 bits.	Key size is 128, 192, 256 bits.	Key size is more than 1024 bits.
Block size is 64 bits.	Block size is 128 bits.	Block size is at least 512 bits.
Encryption and Decryption is moderate.	Encryption and Decryption is faster.	Encryption and Decryption is slower.
Not secured enough.	Secure.	Less secure.
Power consumption is low.	Power consumption is low.	Power consumption is high.
Total number of rounds required is 16.	Total number of rounds required is 10/12/14.	Total number of rounds required is 1.

AES algorithm is a more secure technique than other existing cryptographic techniques. Encryption and Decryption are faster. DES divides the block into two parts before the encryption whereas AES involves a series of substitution and permutation steps to create the encrypted block. The encrypted block is more secure. Therefore, AES can be used to develop more secure system for stored information in the cloud network.

V. LITERATURE SURVEY AND REVIEW

In [1] authors have proposed a verification technique for present location of the data. In [2] authors have explored the security issues within IaaS cloud model.

An overall survey on the security issues and their remedy has been authored in [3]. There authors have also performed a parametric comparison Of the threats, various intrusion detection and their prevention frameworks. In [4] we can see the methodology of modern and classical cryptographic algorithms to provide data security in a cloud environment. In [5] some major security issues of current cloud computing environments have been proposed. In [6] we can see the brief methods, techniques, and best practices for the requirement engineering and management as an emerging cloud service. An attribute-based encryption method was implemented efficiently for critical cloud applications in [7]. In [8] an exhaustive study has been carried out on the security issues and risks in the service delivery model of a cloud computing system. In [9] authors have focused on the security issues related to the service models of cloud computing and the solutions as well. In [10], authors have presented a solution - Security Diagnosis as a Service (SDaaS) for cloud SaaS applications. The research has been carried out thoroughly about an identity and access management in cloud environment [11]. Authors have designed and implemented a framework using unique authentication method to authenticate the legitimate user in [12]. A novel efficient cryptography algorithm has been developed to enhance data security in the cloud in [13]. In [14] researchers have analyzed the security issues of the data storage in the cloud. In [15] researchers have proposed Central Controller device that keeps track of the status of all other devices during the communication by scanning those devices dynamically. Security as a Service model has been proposed in [16]. In [17], authors have described the security issues and future challenges in cloud service authentication. Data storage security in cloud has been explained using AES in [18], [19], [20]. The work on security algorithms has been published in [21]. In [22] authors have carried out the research work on the secure cloud storage using AES.

VI. PROPOSED WORK

We have proposed the verification procedure to enhance the security in Cloud Computing. People from various countries have a UID by which he/she can be identified uniquely. The UID can be used to enhance the security of the cloud network. The UID can be sent via secure gateway to site A where we can apply AES algorithm to encrypt the UID from its plaintext form to ciphertext. We may add some padding bits to make it more secure while sending from site A to site B. At the Site B, decryption of the ciphertext and authentication check will be performed between decrypted UID and existing UID stored in Information System (Info-Sys) [Fig. 5]. Info-Sys is a physical machine installed in site B that keeps personal information of all users of an organizational network. It also manages session for all users in the network. The user can be verified by the Info-Sys only if the UID matches otherwise he/she can never be allowed to enter the system and access confidential data. Info-Sys in Site B also keeps track of all user sessions and security enhances one step further [Fig. 4]. No user will share their UID as it may lead to potential threat for his/her career and living also.

The algorithm is discussed below to show how the Info-Sys helps to enhance top level security in the cloud network.

A. Proposed Algorithm

Step 1: Users generate UID to get access over sensitive information from the cloud network.

Step 2: In Site A,

UID will be converted from plaintext to ciphertext using AES algorithm which include,

- Byte substitution
- Shift rows
- Mix columns
- Add round key

Step 3: In Site B,

The reverse order of encryption will be followed to get the plaintext from ciphertext,

- Add round key
- Mix columns
- Shift rows
- Byte substitution

In this site, the Information System (Info-Sys) authenticates the users by checking the UID provided by them and information that is already stored inside it. If the user is validated by the Info-Sys, then that user can access sensitive information from a website belonging to the cloud network.

Fig. 3 shows the system flowchart to explain the overall functionalities of our proposed system.

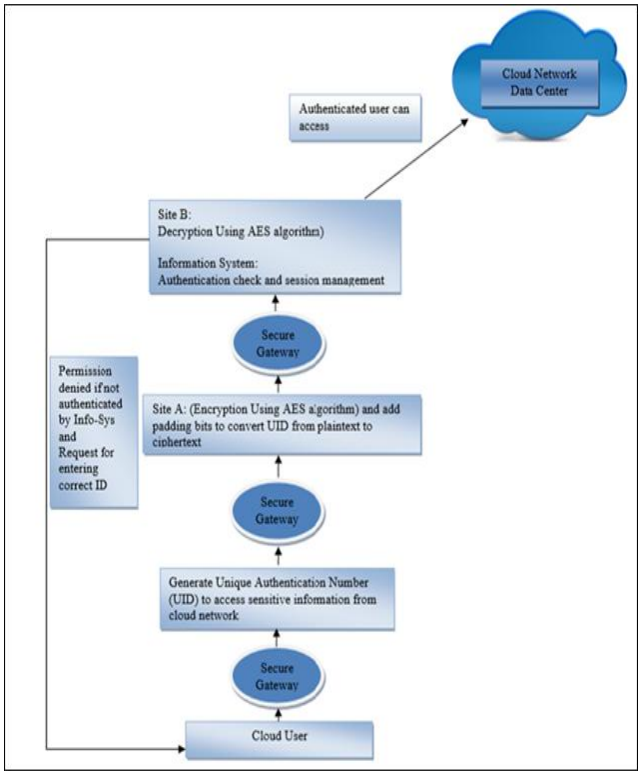

Fig. 3.Flow chart of Security as a Service by verification

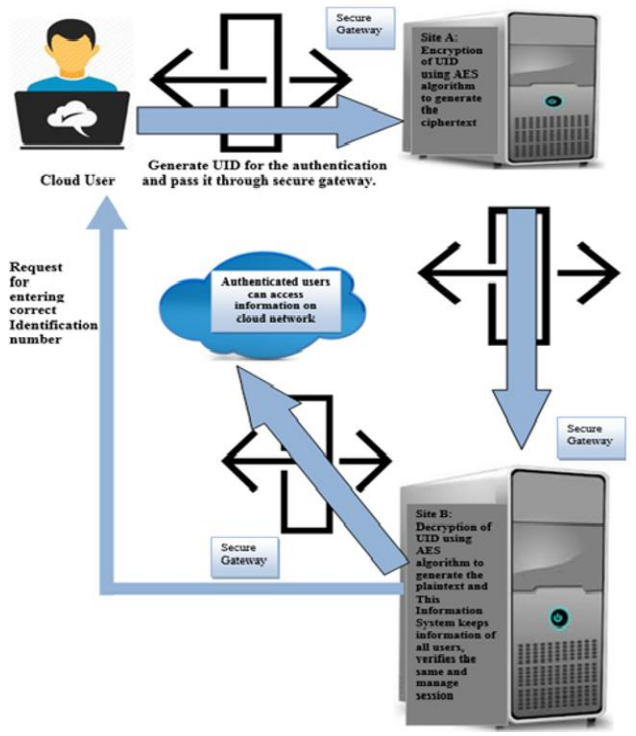

Fig. 4.Security as a Service by verification

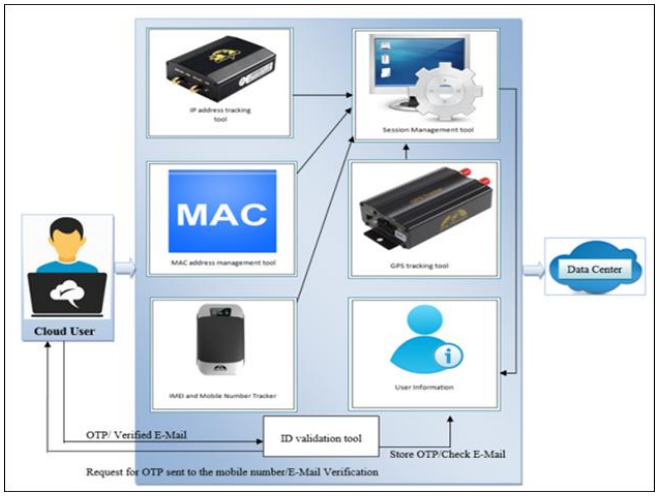

Fig. 5.Info-Sys System Architecture

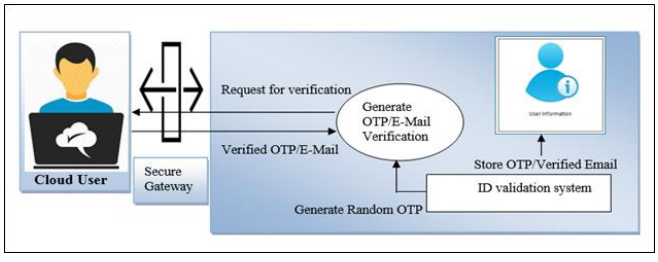

Fig. 6.ID validation tool System Architecture

The security analysis can be done with existing security frameworks. We have applied AES algorithm that enhances the security of the cloud network. The ID is secured as it passes through the secure gateway.

In site A, the UID being a string or a long integer number is converted from its plaintext format into ciphertext using AES algorithm.

In site B, decryption is performed to obtain the original plaintext from ciphertext. During encryption process, all the steps of encryption are performed in reverse order using the AES algorithm.

Info-Sys is present in this site and that checks the validity of the obtained plaintext with the original UID. If it is valid then the person will be eligible to access the information from the secure portal or any organizational website.

Our proposed work focuses on the apex security of the cloud network. Data security, authentication and access rights can be achieved from our proposed system. Web contents and web sites can be made more secure by enforcing UID along with the user id and password.

More secure algorithm, AES is used to encrypt the UID so that it can never be breached easily. Info-Sys is a multi-objective tool that has several functionalities of verification and validation of all users of the cloud network. The proposed work of cloud security also focuses on the access rights of cloud data and at the same time trespassers can be prohibited to access secure data from the cloud net.

B. Different Web Attacks and importance of proposed technique to eliminate them

There are different web attacks. Following are most common attacks that hamper the security of web contents

- Cross site scripting (XSS)
- SQL injection
- DDoS attacks
- Cookie poisoning
- Man in the middle attack
- Wrapping attacks.

These attacks can be handled and prohibited by our proposed system as UID is mandatory for each login [Fig. 7]. UID is very secure, so no person will share it. Info-Sys keeps track of the machine address, IMEI, IP address, user information, user location and used session etc. for every successful and unsuccessful login [Table- II], [Fig. 8]. ID validation tool of Info-Sys also sends the OTP in the mobile number and email specified by the authorized user. The user will be informed about the use or misuse of his/her UID during each successful or unsuccessful login.

Thus, Info-Sys keeps an eye on the authorized user performing illegitimate activities in the cloud or authorized user access, but any person dishonestly steals anyone's UID. If anyone does not share the OTP with the unauthorized person within the time specified, the login for that user will be automatically blocked [Fig. 6]. The proposed system is more reliable. Integrity and confidentiality hold as data is kept secure within the server. Info-Sys has the capability to store and detect the complete information of all users of the system. It will not allow any unauthorized changes on the web contents.

VII. RESULT AND DISCUSSION

We have tried to capture the various aspects of Info-Sys with the suitable pictures below. Info-Sys is implemented with all its functionalities as proposed in this paper beginning from the login page [Fig.7].

Figures show the user information and the session details for all the users who all are already logged into the system and who all are also not able to log into the system [Fig.8], [Fig.9], [Table- II], [Table- III].

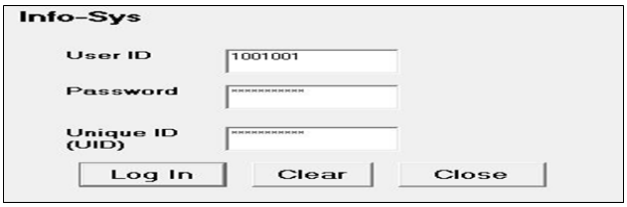

Fig. 7.Info-Sys: user login

Fig. 8.Info-Sys: User Information and Session control

user_id	password	uid	encryptuid	ipaddress
1001001	infosys1001	NYC-G1-3478	S6y6nP+nSDT6:	192.168.42.162
1001002	infosys1002	HBK-G2-2356	aXPUZlMTpDCt	192.168.42.170

datetime	lastlogin	macinfo
04-May-18 7:22:36 PM	04-May-18 6:45:45 PM	Realtek RTL8168D/8111D Family PCI-E
04-May-18 7:30:36 PM	04-May-18 6:48:00 PM	Realtek RTL8168D/8111D Family PCI-E

Fig. 9.Info-Sys Data Store

Table- II. User Information in Info-Sys

UID	Username	Address	Contact Number	Email Id
NYC-G1-3478	John Smith	New York City	1-718-878-5642	john@abc.com
HBK-G2-2356	Allex Gibson	Hoboken	1-201-420-3624	allex@xyz.com

Table- III. Implementation Result

PlainText	Encrypted Text	Key (128 Bits)	Decrypted Text	Code Match
NYC-G1-3478	S6y6nP+nSDT6xfkKXyLcKA==	abcdefghijklmnopqr	123457890123	Yes
HBK-G2-2356	aXPUZlMTpDCbXJOWse7MqQ==	abcdefghijklmnopqr	452535654589	No

VIII. CONCLUSION

Encryption process has long been used to streamline the secure data communication and data security worldwide. An exhaustive study has been made on the existing encryption techniques like AES, DES and RSA algorithms and it has been found that AES is the most suitable algorithm in terms of speed and security. Here, in our work, UID of a user of the cloud network has been encrypted with AES algorithm. The proposed procedure will enhance the security of the network. Our concept can ensure that the Government websites that have secure information of a country, few social networking sites, army base information, IT and corporate information will be secured from the eavesdroppers of other country.

A further research work can be carried out to identify the sleeper cells and the hackers who reside in our globe as common country folks but spread harm over the network due to some self-interested profit-making activities and spoil the access of other users of cloud. Additionally, our prime objective is to bring the completeness of our Info-Sys by incorporating various functionalities which could be much more reliable in future.

APPENDIX

AES- Advanced Encryption Standard
UID- Unique Identification Number
XSS- Cross-site scripting
OTP- One Time Password
DES- Data Encryption Standard
RSA- Rivest Shamir Adleman

ACKNOWLEDGMENT

I would like to convey my hearty respect and sincerest gratitude to my respected research advisor Asst. Prof. Dr. Debabrata Sarddar for sparing his valuable time and assimilating new flawless ideas at every stage of my work. Without his kind co-operation, motivation, and careful guidance, I would not have been able to carry out this research work successfully.

REFERENCES

1. Kumar P R, Herbert Raj P, Jelciana P. Exploring Data Security Issues and Solutions in Cloud Computing. 6th International Conference on Smart Computing and Communications, ICSCC, Elsevier, Procedia Computer Science, 2018, pp.691-697.
2. Chawki Balmany E., Ahmed A., Zakariae T. IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors. The 2nd International Workshop on Big Data and Networks Technologies (BDNT'2018), Elsevier, Procedia Computer Science 134, 2018, pp.328-333.
3. Minhaj A. K. A survey of security issues for cloud computing. Journal of Network and Computer Applications, 71(C), 2016, pp. 11–29.
4. Goodarzi K., Karimi, A. Cloud Computing Security by Integrating Classical Encryption. International Conference on Robot PRIDE 2013-2014 - Medical and Rehabilitation Robotics and Instrumentation. ConfPRIDE, Procedia Computer Science, 42, 2014, pp.320-326.
5. Krishna H. B., Kiran S., Murali G. Security Issues in Service Model of Cloud Computing Environment. International Conference on Computational Science, Procedia Computer Science, 87, 2016, pp.246-251.
6. Ramachandran M. Software security requirements management as an emerging cloud computing service. International Journal of Information Management, 36, 2016, pp.580-590.

7. Kumar N. S., Rajya Lakshmi G.V. Balamurugan B.: Enhanced Attribute Based Encryption for Cloud Computing. International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science, 46, 2015, pp.689-696.
8. Subashini, S., Kavitha, V. A survey on security issues in service delivery models of cloud computing. International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science, 46, 2015, pp. 689-696.
9. Hepsiba, L. C., Sathiaseelan, R.G.J. Security Issues in Service Models of Cloud Computing. International Journal of Computer Science and Mobile Computing, IJCSMC, 5(3), 2016, pp.610-615.
10. Elsayed, M., Zulkernine, M. Offering Security Diagnosis as a Service for Cloud SaaS Applications. Journal of Information Security and Applications, 2018, pp.32-48.
11. Indu, I., Rubesh Anand, P.M., Vidhyacharan, B. Identity and Access Management in Cloud Environment: Mechanisms and Challenges. Engineering Science and Technology, an International Journal, 2018, pp.574-588.
12. Chean L. T., Ponnusamy V., Fati S. M. Authentication Scheme using Unique Identification method with Homomorphic Encryption in Mobile Cloud Computing. 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), IEEE, 2018, pp.195-200.
13. Dash K. S. Panigrahy, C. Simulated Cryptography Algorithm for Enhanced Security of Cloud Data. International Journal of Computer Applications, 109(15), 2015, pp.5-8.
14. Gaur T., Kharb N. Security of Data Storage in Cloud Computing. International Journal of Computer Applications, 110(10), 2015, pp. 15-18.
15. Sarddar, D., Sen, P.; Sanyal, K. M.: Central Controller Framework for Mobile Cloud Computing. International Journal of Grid and Distributed Computing, 9(4), 2016, pp.233-240.
16. Varadharajan V., Tupakula U. Security as a Service for Cloud Environment. IEEE Transactions on Network and Service Management, 11(1), 2014.
17. Lim, S. Y., Kiah, M. L. M., Ang, T. F. Security Issues and Future Challenges of Cloud Service Authentication. Acta Polytechnica Hungarica, 14(2), 2017, pp.69-89.
18. Tamilselvi S. Data Storage Security in Cloud Computing Using AES. International Journal of Advanced Networking & Applications (IJANA), 8(5), 2017, pp.124-127.
19. Akhil K. M., Praveen Kumar M., Pushpa B.R. Enhanced Cloud Data Security Using AES Algorithm. International Conference on Intelligent Computing and Control, 2017, pp.1-5.
20. Arul Jothy K., Sivakumar K., Delsey M. J. Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm. International Journal of Computer Science and Information Technologies, Vol. 8(6), 2017, pp.582-585.
21. Bhardwaj A., Subrahmanyam GVB., Avasthi V., Sastry H. Security Algorithms for Cloud Computing. International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science, 85, 2016, pp.535-542.
22. Babitha M.P., Ramesh Babu K. R. Secure Cloud Storage using AES Encryption. International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016, pp. 859-864.

AUTHORS PROFILE

Debabrata Sarddar, is an Assistant Professor in the Department of Computer Science and Engineering, University of Kalyani, West Bengal, India. He obtained Ph.D. from Jadavpur University. He received M.Tech. in Computer Science & Engineering from DAVV, Indore in 2006, and B.E. in Computer Science & Engineering from NIT, Durgapur in 2001. He published more than 200 research papers in various journals and conferences. His research interest includes wireless and mobile system and Cloud computing.

Sougata Chakraborty, is a Senior System Engineer at IBM India Private Limited in Kolkata, He received M.Tech. in Computer Science & Engineering from Jadavpur University in 2011. He also received B.Tech. in Information Technology from Murshidabad College of Engineering & Technology under West Bengal University of Technology in 2008. His research interest includes Cloud Computing and Mobile Computing.