ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

Researched on Security Challenges with Possible Solution Strategies in Cloud Computing

Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin

Abstract*— The Uses of Information Technology in day-to-day activities, the necessity for online services such as storage space, software, platforms is generating rapidly. This trend to generate a new concept of Cloud Computing. Security of the Cloud Storage is the major concern of cloud computing. When it appears to security of the data stored in the Cloud Storage, it is totally in the hands of the Cloud Providers. The consumer has no contribution in securing the data. In this paper we discuss the various security issues such as Data Access Control, Data Integrity, Data Theft, Data Location, Privacy Issue, Abuse and illegal Use of Cloud Computing, Malicious Insiders, Also we discuss about various techniques like Security Audit as a Service (SAaaS) architecture, TVDSEC, ISO/IEC 27001, Trust_Token protocol, Host Identity Protocol (HIP) to lessen security concerns in cloud computing and different Cryptographic algorithms such as DES, AES, MD5, Blowfish algorithm, RSA to secure data in cloud with some key exchange procedures such as Diffie-Helman Key Exchange technique.

***Index Terms*— Cloud computing, cloud model, security issues, cryptography algorithms, key-Exchange.**

I. INTRODUCTION

Cloud computing is a new term of internet-based computing in which a large number of remote servers are networked to permit sharing of data-processing tasks, centralized data storage, and online access to computer services or resources. It is a combination of hardware and software resources led by third-party services to provide access to developed software applications and high-end networks of server computers and to describe a variety of computing concepts. It relies on sharing computing resources and involves a large number of computers that are connected through a real-time communication network. Cloud computing means a network-based computing, where a program or application has the ability to run on many connected computers at the same time. There are three sensitive states [1] that are of particular concern within the operational concept of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The transmission of clients' own data in cloud servers which are remote server.

All the above three scenarios of cloud computing are strongly prone to security breach that makes the research and inspection within the security perspective of cloud computing practice an imperative one.

The rest of the paper is organized as follows: Section 2 describes the model of cloud computing, various security issues in cloud computing are given in section 3. In section 4 describes different strategies which are used in cloud computing for security purposes along with some cryptography algorithms. Section 5 explains the conclusion.

A. Key Characteristics of Cloud Computing

- Data stored on the cloud.
- Software and services on the cloud.
- Broad network access on the cloud.
- Accessible from any devices.
- Advance security technologies.

B. Advantages of Cloud Computing

- *Fast application deployment*
- *Platform independent, security, scalability*
- *Backup and recovery*
- *Easy access to information*
- *Almost unlimited storage*

II. MODELS OF CLOUD COMPUTING

There are two categories model of Cloud Computing.

A. Deployment Models

The cloud of deployed model may be private, public, community and hybrid. Private cloud is being used by an organization and/or its customers, who owns it whereas public cloud is available for public use. Community model is for a community of users having same purpose. Hybrid model of cloud combines the properties of any of the above models.

B. Delivery Models

The cloud offers its services in the form of software, platform and infrastructure. Costly applications like ERP, CRM etc. will be unloaded onto the cloud by provider. They run at providers Platform includes the languages, libraries etc. The operating system, database, network bandwidth etc. comes under infrastructure. There are three types of cloud delivery models.

Software as a Service (SaaS): In this model cloud server provides different services to the customers according to their requirements.

Platform as a Service (PaaS): It allows platform access for clients as they can put their own software's and applications on to the cloud.

Infrastructure as a Service (IaaS): It provides customers different resources in cloud such as storage, rent processing, network capacity and connectivity.

III. SECURITY ISSUES ON CLOUD COMPUTING

A. Cloud Security on Layered framework

A layered framework is obtainable that assured security in cloud computing environment. It forms of four layers as shown in Figure 3 [2].Secure virtual machine layer is first layer. Second layer is cloud data layer. Third layer is a cloud storage infrastructure layer which accumulates resources from multiple cloud service providers to create a massive virtual storage system. The last layer is virtual network monitor layer, this is the combination of both hardware and software solutions in virtual machines to control problems.

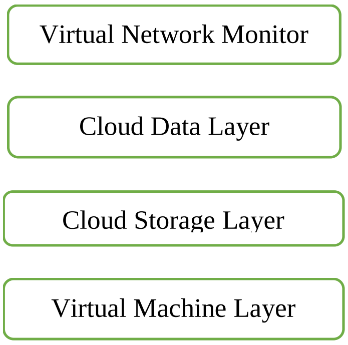

Fig. 3. Layered Framework of Cloud Security

B. Cloud Components Affecting Security

There are different cloud components [2] security issues for cloud computing as it encompasses many technologies including memory management, concurrency control, load balancing, transaction management, Vendor Lock-in [3], cloud networks, resource allocation, virtualization, operating systems and databases. If the vendor closes due to financial or legal problems there will be a loss of data for the consumers. The customer's won't be able to access those data's because data is no more available for the consumer as the vendor shut down. The hypervisor technology is thought as the base of cloud infrastructure. Various virtual machines co-hosted on one physical server by using both CPU and memory resources which are virtualized by the hypervisor. This problem covers the failure of mechanisms isolating attack could be occurred on a hypervisor to achieve illegal access to other virtual machines' memory.

C. Security Faced by Cloud Computing

1. Data Access Control: Sometimes secret data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud environment arise as major issues with regard to security in a cloud based system.
2. Data Integrity: Data integrity includes the following cases, when some human error occurs when data is entered. Errors may occur when data is transmitted from one device to another, otherwise error can occur from some hardware malfunctions, such as disk crashes.
3. Data Theft: Cloud computing uses external data server for cost saving and flexible operation. So there is a possibility of data can be stolen from the external server.
4. Data Loss: Data loss is a very sensitive issue in Cloud computing. If merchandise and banking transactions, research and development information are all taking place online, unrecognized people will be able to access the information shared. Even if everything remains secure what if a server goes down or crashes or attacked by a virus, total system would go down and possible data loss may occur.
5. Data Location: Customers do not always aware the location of their data. Cloud Computing supports a high degree of data mobility. Data might be located anywhere in the world.
6. Privacy Issue: Security of the Customer Personal information is very important in case of cloud computing. Maximum servers are external, so the provider should make sure that is well secured from other operators.
7. Security Issue in Provider Level: A Cloud is well only when there is a better security supported by the provider to the customers. Provider should build a better security layer for the users .And should make sure that the server is well secured from all the outside threats it may come across.
8. User Level Issue: User may be sure that because of its self-action, there would not be any misuse of data or hampering of data for other users who are using the same Cloud.
9. Infected Application: If the service provider have the full access to the server for the view of monitoring and maintenance of server with all rights. So this will protect any malicious user from uploading any affected application onto the cloud which may severely affect the customer and cloud computing service.
10. Availability: Availability is the most significant issue in several organizations facing downtime as a major issue. It relies on the agreement between vendor and the client.
11. Segregation**:** One of the major properties of cloud computing is multi-tenancy [10]. As multi-tenancy permits to store data by multiple users on cloud servers there is a chance of data intrusion. By injecting a client code or by using any application, data can be intruded. So it is essential to store data separately from the remaining customer's data.
12. Abuse and illegal Use of Cloud Computing: The cloud computing supplies an illusion of unlimited computing resources to its users. Anyone can register and start exploiting the cloud services. This is easy for the wrong-doers namely, malicious insiders, spammers and other criminals that can execute their activities within this anonymity of registration [11].
13. Insecure Interfaces and APIs: The cloud communicates with its customers with the help of APIs. The security and availability of cloud services relies on these APIs. Insecure interfaces may occur to dire consequences.
14. Malicious Insiders: A malicious insider [11] in an organization can lead to its destiny. A provider may not reveal how it accept employees' access to physical and virtual assets, how it analyses and reports on policy agreements or how it monitors these employees. The clearness between cloud provider and cloud customer depends on this situation.
15. Unknown Risk Profile: Cloud computing minimizes the hardware and software ownership and maintenance to permit companies to focus on their core business. The security policies may be clearly stated by the service provider to its customer.
16. Loss of Governance: In a public cloud deployment model, customers give up control to the cloud provide over a number of issues that an infect security. Although cloud service provider contracts may not offer commitment to resolve such issues on the part of the cloud provider, thus gives up gaps in security defenses.
17. Responsibility Ambiguity: Responsibility [8] over perspectives of security may be split between the provider and the customer, with the potential for essential parts of the advocacy to be left improvident if there is a failure to allocate responsibility clearly.

18. Authentication and Authorization: The reality that sensitive cloud resources are accessed from anywhere on the Internet heightens the need to build with certainty the identity of a user especially if users now include customers, partners, contractors and employees. Strong authentication and authorization becomes a major concern.
19. Isolation Failure: Multi-tenancy and shared resources are defining properties of public cloud computing. This risk category cover the failure of mechanisms dividing the usage of storage, routing, memory and even reputation.
20. Management interface vulnerability: Interfaces to conduct public cloud resources (such as self-provisioning) are generally accessible through the Internet. Since they permit access to larger sets of resources than traditional hosting providers, they hold on an increased risk, especially when accumulated with remote access and web browser vulnerabilities.

D. Legal Issue in Cloud Computing Contracts

1. Shared Technology Issues: Cloud computing is risen on virtualization. A cloud client has no clue as to which continent or which physical location his data is stored. Each country has its own security policy. For this reason, attackers focus on how to impact the operations of other cloud users and how to achieve unrecognized access to data.
2. Compliance and legal risks: The cloud customer’s investment in gaining certification (e.g., to exhibit compliance with industry rules or standards requirements) may be lost if the cloud provider cannot support evidence of their own compliance with the topical requirements, or does not grant audits by the cloud customer. The customer must monitor that the cloud provider has appropriate certifications in place.

E. Protection Information

1. Privacy: Security of the Customer private information is very important in case of cloud computing. Majority of the servers are external, so the provider should make sure that is well secured from other operators.
2. Compensation for data loss: In the technical or operator error as well as fire or other disasters there may be a possibility that data may be permanently lost by a cloud services provider. Misuse of data by external parties has the hazard of data change.
3. Application Protection: Usually, applications have been secured with defense-in-depth security solutions based on a clear border of physical and virtual resources, and on trusted zones. With the agency of infrastructure security liability to the cloud provider, organizations need to review perimeter security at the network level, employing more controls at the user, application and data level.
4. Data Protection: The major concerns are revealer or release of sensitive data and the loss or unavailability of data. It can be difficult for the cloud service customer to effectively find out the data handling practices of the cloud provider. This problem is bothered in cases of multiple transfers of data.
5. Bad Integration: Migrating to the cloud means moving large amounts of data and main configuration alternatives (e.g., network addressing). Migration of a part of an IT infrastructure to an exterior cloud service provider needs profound changes in the infrastructure design (e.g. network and safety policies). A bad integration occurred by incompatible interfaces or inconsistent policy inducement may evoke both functional and non-functional impacts.

F. Liability

1. Insecure and Incomplete data deletion: The closing of a contract with a provider may not consequence in deletion of the customer’s data. Backup copies of data usually remain, and may be mixed on the same media with other customers’ data.
2. Visibility and Audit: Some enterprise users are creating a shadow IT by following cloud services to build IT solutions except clear organizational approval. Main challenges for the security team are to know about all purposes of cloud services inside the organization (what resources are being used, to what extent, and by whom), understand what laws, regulations and policies may apply to such uses, and regularly assess the security aspects to such uses.
3. License Risks: Software licenses are specially based on the number of installations or the numbers of users. Since developed virtual machines will be used only a few times, the provider may have to attain from more

licenses than really essential at a given time. The deficiency of a clouded license management scheme that permits to pay only for applied licenses may reason software use conflicts.

4. Loss of Trust: It is sometime impossible for a cloud service user to identify his provider's trust level because the black-box feature of the cloud service. There is no standard how to gain and distribute the provider's security level in formalized manner. Furthermore, the cloud service users have no capabilities to appreciate security implementation level achieved by the provider. Such a shortage of sharing security level in view of cloud service provider will become a critical security threat in use of cloud facilities for cloud service users.

G. Performance Management

1. Service levels: Service levels ensures that a provider meets the level of service expected by the agency. This is especially important where the cloud computing service is critical either to the functioning of an agency or to the agency's clients [6].
2. Deficiency of Information/Asset Management: When applying to use Cloud Computing Services, the user of cloud service will have high concerns on lack of information/asset management by cloud service providers such as absence of physical control for data storage, stability of sensitive information, , authenticity of data backup, Disaster Recovery and so on [7]. Yet, the cloud service users also have important concerns on expression of data to foreign authority and on compliance with privacy law such as EU data protection directive.

IV. SOLUTION STRATEGIES IN CLOUD COMPUTING

A. Different Policies and Protocol used to solve cloud security issues

There are various cloud security solutions, that providers should maintain security of data and services when they provides their services to cloud service user in a public cloud solution.

Trust between the Service provider and the consumer is one of the major topic cloud computing. Service Level Agreement (SLA) is the only legal record between the customer and service provider that contains all the treaties between the customer and the service provider; it mentions what the service provider is providing services and is willing to do. In [9], Security Audit as a Service (SAaaS) architecture is proposed which is a cloud survey method and its goal is to extend trust in cloud infrastructures by hiding trifles of what is occurring in cloud from user and cloud provider.

Udaya al. [8] explores the security issues respecting to TVD and suggest few security measures to deal with the attacks in TVD. Some techniques to ensure security in TVD are proposed**.** TVDSEC is a technique uses various components to protect the attacks in the TVD-LAN. Trust enriched security architecture for cloud is proposed in this method [10].

Legal Issues is also one of the important issues, the laws vary from country to country, and customer have no control over where their data is physically stored. Regulatory measures such as, privacy and data security laws and rules that cloud systems need to observe. Before migrating applications or data to a cloud computing environment, it is essential to understand exactly the specific laws or regulations that apply and the topical duties or obligations assigned on both the customer and the provider.

The most globally recognized international standard for information security compliance is ISO/IEC 27001 [11] which contains national variants and well developed certification regimes. ISO has new standards, ISO/IEC 27017 [14] "Code of practice for information security controls based on ISO/IEC 27002 for cloud services" and ISO/IEC 27018 [14] "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" which generally use in cloud service security and privacy considerations and which build upon ISO/IEC 27001.

In IDM (Identity management) system [13] is proposed which has the capability to use identity data on untrusted hosts. This method uses the predicates over encrypted data and multi-party computing for the use of a cloud service. It creates active middleware agent that contains privacy policies, a virtual machine that enforces the policies, and has a set of protection appliances to protect itself. An active agent interacts in the location of a user to authenticate to cloud services using user's privacy mechanisms. The security issues in an Infrastructure-as-a-Service (IaaS) cloud service model connected with the virtual machine (VM) migration [14] from one cloud platform to the other cloud platform. A protocol called “Trust_Token” is developed which ensures that the user VM can only be migrated to a cloud platform which is trustable.

A process called SVA (Security Vulnerability Assessment) system is used which is a risk-based and performance-based method which includes five steps such as Apply SVA Tools, Assessment Report, Vulnerability Analysis, Risk Assessment, Counter measures Analysis[15].

Data Splitting is a solution for cloud security issues. Here the data split over multiple servers or hosts that cannot communicate with each other; only the owner who can permit to access both hosts can collect and combine the separate datasets to recreate the original.

Michael al. suggests a technique to protect cache-based side-channels [22]. This technique is accomplished within the server of a Cloud system and it is performed so that there is no interruption with the Cloud's methods of operation. The solution proposes cache-based side channels in the Cloud and it does not interact with the Cloud model which needs no changes to the client-side feature, or to the underlying hardware.

Be sure to the consumer's access devices or points such as virtual terminals, gazettes, pamphlets, personal computers and mobile phones are secure enough. Access to the unrecognized device by an unauthorized user can cancel even the best security protocols loss of an endpoint access device in the cloud.

A virtualization-aware security solution is suggested in which the security software is installed in a given dedicated and predefined Virtual machine with privileged access to hypervisors to secure other Virtual machines. It is advised to access micro-hypervisor with microkernel to give high level security [15].

In cloud computing Virtualization and SOA technologies is one the main feature [23]. Seven principles of Open Architecture of Cloud Computing such as Cloud Quality and Governance, Virtualization for Cloud infrastructure, Integrated Ecosystem Management for cloud, Extensible Provisioning and Subscription for cloud, Service-Orientation for common, Unified Information Representation and Exchange framework, Configurable Enablement for cloud offerings are described.

Data Access Monitoring have to assure about whom, when and what data is being accessed for what purpose. Cloud service provider must share diagrams or any other information or provide audit records to the consumer or user. Provider must verify the proper deletion of data from shared or reused devices. Cloud service providers must give enough details about fulfillment of promises, break remediation and reporting contingency. Solution for such issues is to use digital signatures.

A CLOUDWATCHER is used to give monitoring services for large and dynamic clouds [30]. The Cloud Watcher automatically identifies the network packets which needs to be inspected by using the pre-installed network security devices. A cloud operator can monitor or examine the cloud easily and efficiently with CLOUDWATCHER and it provides security monitoring as a service to all its tenants. CLOUDWATCHER develop practical and feasible network security monitoring in a cloud network.

Zhidong al. defines the cloud computing security challenges by proposing a solution called the Trusted Computing Platform (TCP) [20]. TCP is used to measure authentication, confidentiality and integrity in cloud computing environment. Trusted cloud computing process is developed by using TCP as the hardware for cloud computing and it assure privacy and trust.

Host Identity Protocol (HIP) [21] is a suggested solution technique which develops a way to authenticate and protect data flows between clients belonging to the same security domain. HIP is experimented in different conditions to solve the multi-tenancy challenges for public and hybrid IaaS clouds. In this system, developers and administrators can use cloud services explicitly over HIP, whereas customers use the cloud without HIP using a reverse HTTP proxy that acts as a load balancer for a distributed test service. HIP was used to secure internal connectivity in the clouds and a load balancer concluded HIP tunnels towards end-users.

B. Different Cryptographic Algorithms

Preserving confidentiality and Integrity is a major issue. Data encryption prohibiting the improper disclosure of information. Encryption is suggested as a good solution to secure information. Before storing data in cloud server it is better to encrypt data. Data Owner can give access to particular group member such that data can be easily used by them. A data security model consists of authentication, data encryption and data integrity, data recovery, user protection has to be planned to improve the data security over cloud. To assure privacy and data security data safeguard can be used as a service. To escape access of data from other intruder, applying encryption on data that transmits data entirely unusable and normal encryption can complicate availability. At first before uploading data into the cloud the users are advised to verify whether the data is stored and the keywords in files remain unchanged. There are some algorithms used for the encryption purpose which are mentioned below:

1. **Symmetric (secret) Key**: This cryptographic method makes use of two different algorithms for encryption and decryption respectively, and a key that is shared between the sender and the receiver. The original data or message is known as plaintext and the encrypted data or message is known as the cipher text. Sender uses the encryption algorithm and a key to transfer a plaintext into a cipher text and sends through a medium. The receiver transfers the cipher text into a plaintext using a decryption algorithm and the same key that was used for encrypting the message.

Encryption: C=Ek(P) Decryption : P=Dk(C)
And
Dk(Ek(x))=Ek(Dk(x))=x

1.1 DES

DES is a symmetric key block cipher that is applied to encrypt/decrypt 64 bits of a block data. The encryption method is made up of two permutations known as the initial and the final permutation and sixteen Fiestel rounds.

1.2 AES

AES is also a symmetric-key block cipher that is applied to encrypt/decrypt a data block of 128 bits. The size of the key in AES can be 128, 192 or 256 bits, relying on the number of rounds (10, 12 or 14 respectively). It is a non-Fiestel cipher.

1.2 MD5

MD5 is broadly used cryptographic hash function. The hash value of 128 bit processes a variable length message into fixed length message of 128 bits. The input message is separated into blocks of 512 bits. The message is also encrypted so that its size is divisible by 512 public key of the receiver is used for encryption and private key of receiver is used for decryption [21].

1.4 Blowfish algorithm

It is a symmetric block cipher algorithm. It is used for the methods where the keys not change frequently. The block length for blowfish is 64 bits. When performed in 32 bit microprocessor with huge data caches this algorithm is taken into most appropriate. Data encryption flows through 16 rounds of fiestal network [17].

2. **Asymmetric (public) Key**: This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a separate key for encryption and another a separate key for decryption. The sender encrypts the message using the public key of the sender. The receiver decrypts the cipher text with the help of a private key.

2.1 RSA

RSA based data integrity check can be provided by conjoining identity based cryptography and RSA Signature. To compute large files with different sizes and to address distant data security RSA based storage security method can be used. RSA [18] is a public key algorithm that uses modular exponentiation for encryption/decryption. It requires two exponents, e and d, where e is public and d is private. To attack it, an intruder needs to calculate $\sqrt[e]{C}$.

2.2 Diffie-Helman Key Exchange

In Diffie-Hellman protocol [19], two parties generate a symmetric session key without the help of a Key-Distribution-Center (KDC). Before to create a symmetric key, the two parties need to choose two separate numbers p and g. These two need not be confidential. They can be public, means these can be sent through the Internet.

V. CONCLUSION

Although cloud computing is the new arising technology that presents a good number of benefits to the users, it faces lot of security challenges. Main purpose of cloud computing is to securely store and manage the data in cloud. In any cloud system (Infrastructure, software or platform) the end service provider control the access to the services. As these services are being provided or hosted on cloud so the cloud provider needs to protect their network from unauthorized accesses. In this paper, firstly we described different types of security issues for cloud. These issues include storage security, network security, data security and application security. Secondly, we discussed different methods which have been used to solve these security challenges. Also we described various encryption and decryption algorithms which ensure privacy and data security in cloud. To ensure the security of data access in cloud advanced encryption procedures can be used for storing and retrieving data from cloud. Proper key management systems also ensure the distribution of key to the cloud users as only authenticated persons can access the data.

REFERENCES

[1] Monjur Ahmed and Mohammad Ashraf Hossain. "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD" International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[2] “Negotiating the cloud – legal issues in cloud computing agreements Commonwealth of Australia 2012”, ISBN 978-1-922096-05-0.

[3] “Security for Cloud Computing Ten Steps to Ensure Success Version 2.0”, Copyright © 2015 Cloud Standards Customer Council.

[4] Anitha Y, “Security Issues in Cloud Computing - A Review”, International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.

[5] R. Velumadhava Rao, K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing”, International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015).

[6] Tania Gaur, Nisha Kharb, “Security of Data Storage in Cloud Computing”, International Journal of Computer Applications (0975 – 8887) Volume 110 – No. 10, January 2015.

[7] Negotiating the cloud – legal issues in cloud computing agreements Commonwealth of Australia 2012, ISBN 978-1-922096-05-0.

[8] Kangchan Lee, “Security Threats in Cloud Computing Environments”, International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[9] Udaya Tupakula Vijay Varadharajan, “TVDSEC: Trusted Virtual Domain Security”, Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference, Victoria, NSW, 5-8 Dec. 2011, pp 57–64, Print ISBN: 978-1-4577-2116-8, DOI: 10.1109/UCC.2011.18.

[10] Frank Doelitzscher∗, Christian Fischer∗, Denis Moskal∗, Christoph Reich∗, Martin Knahl∗ and Nathan Clarke, “Validating Cloud Infrastructure Changes By Cloud Audits”, Services (SERVICES), 2012 IEEE Eighth World Congress, Honolulu, HI, 24-29 June 2012, pp 377 - 384, Print ISBN: 978-1-4673-3053-4, DOI: 10.1109/ SERVICES.2012.12.

[11] Vijay Varadharajan Udaya Tupakula, “TREASURE: Trust Enhanced Security for Cloud Environments”, Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 145 – 152, Print ISBN: 978-1-4673-2172-3, DOI : 10.1109/TrustCom.2012.283.

[12] K.Mukherjee, G.Sahoo, ”A Secure Cloud Computing”, International Conference on Recent Trends in Information, Telecommunication and Computing, Mar 12th 2010, Washington DC, pp 369-371, ISBN: 978-0-7695-3975-1, DOI: 10.1109/ITC.2010.95.

[13] Wentao Liu, “Research on Cloud Computing Security Problem and Strategy”, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012, pp 1216-1219, Print ISBN: 978-1-4577-1414-6, DOI: 10.1109/CECNet.2012. 6202020.

[14] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, Mark Linderman, “Protection of Identity Information in Cloud Computing without Trusted Third Party”, Reliable Distributed Systems,

2010 29th IEEE Symposium, New Delhi, Oct. 31 2010-Nov. 3 2010, pp 368 – 372, ISSN : 1060-9857, Print ISBN: 978-0-7695-4250-8, DOI: 10.1109/SRDS.2010.57.

[15] Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, "Security and Trust Preserving VM Migrations in Public Clouds", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.

[16] S C Rachana, Dr. H S Guruprasad, "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967.

[17] Divya saraswat , Dr. Pooja Tripathi , "Cloud Security and Algorithms: A Review", International Journal of Enhanced Research in Science Technology & Engineering, Vol. 3 Issue 10, Oct.-2014, pp: (113-117), Impact Factor: 1.252, ISSN: 2319-7463.

[18] G.Devi, M.Pramod kumar, "Cloud computing: a CRM service based on a separate encryption and decryption using blowfish algorithm", international journal of computer trends and technology, volume 3 issue 4, ISSN: 2231-2803, 2012, pp. 592-596.

[19] Garg, Preeti, and Vineet Sharma. "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function." Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.

[20] Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography." IACR Cryptology ePrint Archive 2014 (2014): 49.

[21] Zhidong Shen, Qiang Tong " The Security of Cloud Computing System enabled by Trusted Computing Technology", 2nd International Conference on Signal Processing Systems, Dalian, (ICSPS), 5-7 July 2010, Vol 2, pp 11-15, Print ISBN: 978-1-4244-6892-8, DOI: 10.1109/ICSPS.2010.5555234.

[22] Miika Komu, Mohit Sethi, Ramasivakarthik Mallavarapu, Heikki Oirola and Rasib Khan, Sasu Tarkoma "Secure Networking for Virtual Machines in the Cloud", Cluster Computing Workshops (CLUSTER WORKSHOPS), IEEE International Conference, Beijing, 24-28 Sept. 2012, pp 88 – 96, Print ISBN: 978-1-4673-2893-7, DOI: 10.1109/ClusterW.2012.29.

[23] Michael Godfrey & Mohammad Zulkernine, "A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud", IEEE Sixth International Conference on Cloud Computing, Washington, DC, USA, pp 163-170, ISBN: 978-0-7695-5028-2, DOI: 10.1109/CLOUD .2013. 21.

[24] Ashutosh Kumar Singh, Dr. Ramapati Mishra, Fuzail Ahmad, Raj Kumar Sagar, Anil Kumar Chaudhary, "A Review of Cloud Computing Open Architecture and Its Security Issues", International Journal Of Scientific & Technology Research, Issue 6, Vol 7, july 2012, pp 65-67, ISSN: 2277-8616.

[25] Seungwon Shin, Guofei Gu," CloudWatcher: Network Security Monitoring Using OpenFlow in Dynamic Cloud Networks", Network Protocols (ICNP), 2012 20th IEEE International Conference, Austin, TX, Oct. 30 2012-Nov. 22012, pp 1-6, Print ISBN: 978-1-4673-2445-8, DOI: 10.1109/ICNP.2012.6459946.

AUTHOR BIOGRAPHY

Md. Alam Hossain, Assistant Professor, Computer Science and Engineering Department, Jessore University of Science & Technology, Bangladesh. His research interests is the security of cloud computing.

Md. Biddut Hossain, MSC Student, Computer Science and Engineering Department, Jessore University of Science & Technology, Bangladesh. His research interests is the security of cloud computing.

Md. Shafin Uddin, MSC Student, Computer Science and Engineering Department, Jessore University of Science & Technology, Bangladesh. His research interests is the security of cloud computing.