International Journal of Grid Distribution Computing
Vol.8, No.2 (2015), pp.155-166
http://dx.doi.org/10.14257/ijgdc.2015.8.2.15

Study on Cloud Security Risk and Remedy

Asish Aich and Alo Sen

School of Comp. Engg., KIIT University
{acrana.dgp09, alosen10}@gmail.com

Abstract

Recently, Cloud computing is most powerful research area because of its flexibility and cost efficiency. The environment provides dynamic, easily scalable services. Although cloud computing promises to the organization as well as consumers to make life much easier, still it has considerable level of security issues. When data is transferred between the client and server, then security is a great concern. Efficient model should be implemented in the cloud environment to make it secure from illegitimate users. So that cloud security is becoming a important recent discussion in the IT sector. This paper describes a survey on different security issues of cloud computing and the possible solution for remediation.

Keywords: *Cloud Computing, Digital Signature, One time Pad, Security risks assessment, Encryption*

1. Introduction

Cloud Computing is a new standard for the organizations to extend their business with small investment on their capital and to provide service over internet. Cloud Computing creates a shared virtual environment for the physical resources and provide the services to the client as Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a service (IaaS) models. The functions of Cloud computing can be enlarged by adding networking which allow the cloud providers to give shared access to network resources along with the other resources. However, the network resources which are added with the existing cloud environment models initiates network-based security challenges. Schoo et al., described some of the security challenges [1] like information security, communication security, and virtualization environment threats.

Security is a great issue for cloud computing. The three main security goals confidentiality, integrity, and availability should be incorporated in the cloud system. For a secure cloud computing protection is needed for user identity, their data, and server data privacy. Data can be stolen during transmission as well as at the time of storing on the server. There are lots of security risks associated with cloud computing. This paper presents a survey on all possible security issues of cloud environment and feasible remediation.

This paper has two sections in addition to introduction and conclusion. Section 2 covers different security issues and possible remedy for it and Section 3 deals with cloud environment security solutions.

2. Cloud Security Issues and Possible Remedy

The communication in cloud environment takes place through the popular TCP/IP protocol that identifies the different cloud providers over the network through IP addresses. A VM (Virtual machine) in the Internet also has an IP address like a physical computer in the Internet. So, for a malicious user it is not a big deal to find this IP addresses. There is an easy way to implement a malicious virtual machine at

ISSN: 2005-4262 IJGDC

the location of the physical server to initiate an attack. As a result, if the attacker can take the control over the VM, then all the legal users who use the same VM will be a victim of that.

2.1. Data Leakage

Description: There is a great chance of data leakage in cloud environment where data moves from a customer's local machine to a fully shared environment. Because of that, Data leakage becomes a vital security risk among different security issues in cloud environment. Data leakage prevention (DLP) applications can be used to prevent the sensitive information. But DLP application can't protect the data confidentiality in all types of cloud. In SaaS and PaaS, The client's data with DLP agents can't be discovered until the provider will put the required feature in its service. In private clouds, Customer can have direct control of the total infrastructure, so there is no concern whether DLP agents are implemented in connection with SaaS, PaaS, or IaaS services. In public cloud, deploying a DLP agent is complex in nature. In hybrid cloud, for IaaS, client can deploy DLP agents for some control over data.

Remedy: Should have to implement API access control strongly. Encryption technique should be enabling to protect data integrity during transit. The protection of data should be analyzed at the time of design as well as run time.

2.2. DDoS Attacks

Description: Distributed Denial of Service attacks make resources or services not available to the customer by flooding them with traffic [2] which is useless for indefinite period of time. The main objective of this attack is, to take control over resources (time of CPU, bandwidth of network) such that it can't give services to the authorized users. The another objective is achieved by hiding the identity through mimicking legal traffic of web service and creation of a large number of agents for initiating an DDOS attack [3, 4]. As a common way of DDoS attack, the attacker hides their identity generally by spoofing the IP address part of a packet header from the victim. For which this is very difficult to trace the origin of an attack. A traditional solution DDoS attack was increasing the number of critical resources. But it is a serious problem when an attacker deliberately done a DDoS attack using botnet with large number of zombie machines. Most network providers cannot protect this attack because they are incapable to distinguish between good traffic from bad traffic.

Remedy: Intrusion Prevention Systems (IPS) can be a solution if the attacks can be identified with pre-existing signatures but is ineffective if there is legitimate content with bad intentions. Like IPS, firewalls are also inefficient against DDoS attacks because firewalls can be bypassed easily.

2.3. Abuse of Cloud Computing

Description: IaaS providers offer unlimited network, storage, and compute capacity for their customers. Sometimes they provide "frictionless" registration process through which those who have a valid credit card can register and begin to use cloud services. Sometimes client get free limited trial periods. By abusing the anonymity through these registration and different models, malicious code authors, spammers have been able to misuse it. Traditionally PaaS providers have been suffered by these types of attacks. Although, current report displays that attackers are targeting to IaaS consumers also. Cloud providers have to be concern about some future areas like cracking of password and key, DDoS, malicious data hosting, launching of dynamic attack points, building of rainbow tables, botnet command, control and CAPTCHA solving farms.

Remedy: There should be strict initial registration with validation processes, enhanced service for coordination and monitoring of credit card fraud, service for monitoring blacklists (public) for one's own network blocks.

2.4. Insecure Interfaces and APIs

Description: Clients use to manage and interact with cloud services through a set of software interfaces or APIs. The services like provisioning, orchestration, management all are performed using the interfaces. The availability and security of cloud services is depend on the security of those APIs. So, the interfaces must be designed in such a way that they will be protected from any accidental or malicious attempt. Furthermore, sometimes third parties build upon those interfaces to offer extra value-added services to their clients. It introduces more complexity of the new layered API; which also increases risk, because organizations may have to communicate with the third parties to enable their agency.

Remedy: Proper analysis of the security model of the interfaces. Ensure that strong access controls and authentication are incorporated with the encrypted transmission.

2.5. Malicious Insiders

Description: This threat is well-known to most organizations. This threat is for the customers for the lack of transparency into cloud provider's process and procedure to the services of IT and customers. For example, a provider sometimes may not reveal about the granting of employees access , the way of monitoring those employees or the way they analyzes and reports on policy compliance. Sometimes there is little or no visibility into the practices and hiring standards for the employees. This type of situation lead to an attractive opportunity for an attacker — ranging from a hacker, to corporate espionage, to organized crime, or even nation-state sponsored intrusion.

Remedy: Should enforce supply chain management strictly and have to conduct a comprehensive supplier assessment as part of legal contracts should specify human resource requirements. Transparency is needed to be maintained in overall information security practices and compliance reporting. Determination of the security breach notification processes is needed.

2.6. Shared Technology Issues

Description: IaaS vendors provide the services by sharing infrastructure in a scalable form. Sometimes, the components of the underlying infrastructure (*e.g.,* CPU caches, GPUs, *etc.*,) are not designed in a way which can offer property of strong isolation for a multi-tenant architecture. For addressing this gap, a virtualization hypervisor incorporated between the operating systems (guest) and the physical compute resources. A depth strategy defense is considered, and it should include storage, computation and enforcement of network security and monitoring. Strong compartmentalization should be incorporated to ensure that each individual client do not affect the operations of other running under the same cloud service provider. One client should not have access to any other's actual or residual data, network traffic, *etc*.

Remedy: Security should be implemented during configuration. Environment activity should be monitored effectively. Powerful authentication and control access should be promoted for the process of administration and activities. Service level agreements (SLA) should be enforced for the remedy of patching and vulnerability. Scanning of vulnerability and configuration audits should have to be conducted.

2.7. Account or Service Hijacking

Description: Attacks like fraud, phishing, and different software vulnerabilities comes under account or service hijacking. Sometimes, passwords and credentials are reused, which leads to such type of attack. In cloud environment if a hacker somehow gets access to the customer's information, then the attacker can easily capture client's information by eavesdropping on their transactions and activities, modify the information, return fabricated data and redirect the clients to unauthorized sites. Then the client's account instances will become a new platform for the attacker and they may use the account to launch the other attacks.

Remedy: Should have restriction for the sharing of credentials of account between services and users. Two-factor strong authentication methods should be implemented where possible. Unauthorized activity should be detected effectively. Cloud provider security policies and SLAs should have to be understood clearly.

2.8. Side Channel Attacks

A malicious user can want to access the cloud environment by putting a malicious VM in close to the targeted cloud provider server and later initiating a side channel attack.

2.9. Man-in-middle Cryptography Attacks

These types of attacks take place while an attacker can intercept and modify the communication take place between two users.

2.10. Security of Network

a. Penetration and analysis of packet in network.

b. Weaknesses in managing the session.

c. Insecure configuration of SSL.

2.11. Security of Web Application

a. SQL, OS and LDAP injection

b. Cross-site scripting

c. Insecure direct object references

d. Broken authentication and session management.

e. Restriction to URL access failure.

f. Redirections and forward is not validated.

g. Cross-site request forgery.

h. Cryptographic storage is insecure.

i. Transport layer protection is not sufficient.

Table 1. List of Different Assessment Report of Security Risk from Different Consumer's Point of View Faced by the Cloud

Serial no	Security risk	Description
1	Regulatory compliance	Cloud environment providers those refuse to security certifications and external audits.
2	Privileged user access	The sensitive information which is executed externally outside the organization leads to risk of security.
3	Location of data	While using cloud environment, customers don't know about the location of the hosted data.
4	Segregation of data	The available information in the cloud is shared totally with the data from the other customers.
5	Recovery	The cloud provider should give information to the customers about their execution of data in the time of failure of the cloud services.
6	Investigative support	Investigation of illegal or inappropriate activity is not possible in cloud environment.
7	Long term viability	The customers should have to be sure that their data will available in a long term basis.

Table 2. List of Major Security Issues in Different Services

Serial no	Services	List of security issues
1	SaaS	• Security of data and network, location of data, integration of data, access to data, segregation of data, authentication and authorization, confidentiality of data, security of web application, breaches of data, vulnerability in virtualization and availability of data.
2	PaaS	• Cloud provider can give control to the user to build application on the top of the platform. But the security provided below the application level (host and network intrusion prevention) still available to the provider. • Enterprise Service Bus (ESB) has to be secure strongly, with protocol like Web Service (WS) Security (Oracle, 2009).The segmentation of the ESBs is impossible in PaaS cloud

		environment. Metric have to be maintained properly for effectively control the different application security programs. • The attacker may attack the available code which is not only the code which runs in user context. Even, they may attack the whole architecture and may do a black box testing. The security risk of cloud is not always attached with the web programs but risk is also associated with the Service Oriented Architecture (SOA) applications.
3	IaaS	• Virtual machines which have critical applications and sensible information, off premise to public and shared cloud environments creates lots of security risks to be resolved for the organizations which rely on network perimeter defense as the proper method to prevent their data centre.

3. Cloud Environment Security Solutions

To maintain the security of our cloud-based virtual infrastructure, perfect application should be implemented in the traditional IT environment as well as in cloud environment. For ensuring the four major security goals (confidentiality of data, authentication of legitimate user, integrity and availability of data) the cloud provider should include the following techniques:

1. Encryption: The sensitive data sensitivity has the requirement of the encryption of the traffic to and from the VM including encryption process to the host OS application.

2. Physical Security: Physical security is possible by keeping the VM and cloud environment hosts secure and safe behind carded doors.

3. Authentication and Access Control: The authentication policy of the VM should have to be similar with physical systems authentication. Biometrics and One time password should have to be implemented in the same way. Again authentication is mandatory while data or message is transferred from one to another cloud. Digital signatures can be used to provide the authentication.

4. Separation of Duties: When system become more complex, then proper configuration can't take place. So cloud providers must have to be sure about the enforcement of least privileges access with accountability and control access.

5. Change control, Configuration and Patch Management: Sometimes, the important three things may be skipped in small organization. Configuration, patch management, change in control and updating of processes have to take care to the cloud world as well as in the real world.

6. Intrusion Detection and Prevention: The network traffic comes and goes out of our network have to be known to us. A host based intrusion detection and prevention system

associated with a hypervisor based solution will be able to examine for virtual network traffic passing through the network.

The Cloud Environment can be Made Secure in the Following Three Ways:

3.1. To Secure the Transmission

The data communications take place between the client and cloud server through the network. Different Malicious flooding routes need to be maintained by setting limitation for each route [5]. The number of packets a route at a time can transfer defines its limit. To maintain security in the transmitted signals different encryption algorithms (public as well as private key encryption), may be used with spread spectrum modulation [6]. Through Wired Equivalent privacy (WEP), SSID for each access point and MAC addresses filtering [7] a wireless transmission can be made secure.

3.1.1. Tunneling: Tunneling make the data secure at the time of transmission. The packet which should be transmitted to the server is encapsulated with a new packet with the address of another node. Then when the packets will reach to that node then it will be directed automatically to the server. This encapsulation prevents the attacker to trace the original packets made for the server thus it reduces the possibility of hacked. The goggle threat hacking can also be reduced by implementing this method [8].

3.1.2. Use of Virtual Circuits: The IP packets move in the form of datagram through the network, so they choose the best possible route. However, it is possible that they may also pass through an already attacked router by an attacker. In such scenario, the packets can be easily exploited and tracked down by the attacker. A virtual circuit can be implemented to prevent this type of attack. In this method, at the time of connection establishment the server sets a fixed route, which the packet should follow. This path is made to have gone through authorized routers. This path insures security on data but in case a router on the path is down, it may fail.

3.2. To secure the Servers

3.2.1. Intrusion Detection System (IDS) : Attack like SQL injection can be monitored using intrusion detection system. IDS keep track of the different possible request from the user and make query to monitor these attacks [9]. It can be treated as an immune system for the system. IDS with soft computing can detect different attacks in the network [10].
An ambiguous behavior can be detected in the network using source and destination IP addresses, port addresses, CPU cycles *etc.* [11]. Sate machine replication help to detect the nodes with abnormal behavior which indicate the attacked nodes [12]. Dynamic source routing based algorithms can be implemented to detect a possible attack for mobile ad-hoc network [13]. Fuzzy networks can also be used to analyze the network [14].

3.2.2. Separate Servers: When multiple applications run on a single server then the load on a server increases and also there is a great chance to be got attacked through different possibilities [15]. While running one application, it can pose a threat to the other applications on that particular server. So the correct way is to store different applications on different servers. This prevents from the arise conflicts but it also increase the cost to set up the servers. Multi threading parallelization can speed up the servers by reducing the response time [16]. Address assignment and resolution problem has been reduced with the introduction of IPV6 [17].

3.2.3. Store Hashed Values: The data in the cloud database is naturally plaintext. Now once the database broke the entire data can be exploited. So, to prevent the exploitation

the hashed value of data can be stored. The key can be stored securely. For each database object (table and view) the hashing key can be generated randomly. Another way is by using the sum of natural numbers or prime numbers embedding the messages to prevent it from distortion [18]. Using grid computing the servers can be more computationally strong. Grid security can be added later for enhancement of the security of the server [19].

3.2.4. Replication: For the availability of data the server should be working all the time without any failure. But in reality it is not possible for a server to give service all the time. The service may be unavailable due to some failure. Replication can handle this type of failure. The replicated server can be used if one server not works properly. Synchronization is a great concern for it. Periodic update can be done to the entire server for keep them up to date.

3.2.5. Threshold for Server Load: The main aim of DOS attack is to crash one server by making it overloaded and thus prevent the legitimate user to access the server. To solve this type of attack a threshold value can be set to limit the load a server can handle maximum [20]. When the maximum threshold value reach for a particular server then the rest of the load get transfer to the replicated servers. Thus the load on a server can be managed properly. Integrity is maintained by locking of data while writing to the same file when request come from both the servers. Flooding request also need to be handled to prevent the server from getting overloaded.

3.3. To Secure the Client

If attribute based encryption and proxy encryption can be combined then client data can be secured. Client's access accounting should be done [21].

3.3.1. Digital Signatures: Digital signature is used for the authentication of the servers but authentication methodology in unavailable to the client side. In cloud environment all of the clients are known previously, so it is easy to identify the clients through digital signatures. Various methods like RSA may also be used. This may increase the time of computation but preserve the security. RSA computation prevent the client machine not to be overloaded due to large storage of the cloud environment [22]. For unique identification, digital water marking can be used [23].

3.3.2. One Time Password: Once an attacker gets access to the user password then he can launch a replay method to attack that system. This type of attack can be handled by one time password. The server generate the password randomly and the password to the client using a secure channel. For each session, client gets a unique password. Another way is to embed the messages with it's redundancy in html pages in case one time password reach to expensive form [24]. One time password also secures the data from cookie because during every session new password is generated thus the stored information in a system cannot be used again [14].

3.3.3. Authentication for Every Write: Authentication before every write should be imposed because it will be stored permanently in the database. So, the client should be authenticated first. Asking for the password before each write ensures that write in a file will be done by an authenticated user only. Multifactor authentication scheme may be used to enhance security [25]. Password hashing methodology can be incorporated to authenticate the users [26].

3.3.4. Distributed Storage: Storing parts of the client's data in different location across the environment is a flexible way. Thus if one location is get attacked then also the client would not lose the whole data. Hence, it can be restoring easily. The client need not know

at which location their data is stored as the whole system is totally location transparent. But the system on the distributed environment should be handled with proper synchronization. Erasure correcting code should be used to secure the data storage [27].

3.3.5. Local Servers: Frequent users have need of only few common applications. So, local server can be used to store that type of applications which will help to get fast access by avoiding network congestion. The session data and template for dynamic documents can be cached to the local servers [28].

3.3.6. Temporary Storing on Local Disk: Another feasible way to minimize the attack is avoiding the constant connection to the internet. It can be possible by storing the file on local disk temporarily for one session and once all the operations of that session is done then update the cloud database [29]. However, This requires larger size of local disk which will be capable enough to store the session's information.

3.4. To Build Secure Cloud

The cloud environment has to be build secure combining different features depending on the level of security needed. Two time authentications can be achieved by combining one time password and digital signature.

4. Conclusion and Future Work

With the ever advanced Technological growth, Cloud Computing model will gradually change the landscape of IT industry. Though, there are several benefits provided by the Cloud environment, security issues are still one of the biggest issue. In this paper, we have surveyed various security issues and existing solutions in cloud computing. A large number of parameters and different types of soft computing techniques can be included in the future to enhance security in cloud environment.

Acknowledgements

The authors are thankful to the anonymous reviewers for their valuable comments and suggestions which improves the presentation of this paper effectively. Authors are also thankful to all of the professors who helped directly or indirectly to work on this paper.

References

[1] P. Schoo, V. Fusenig, V. Souza, M. Melo, P. Murray, H. Debar and D. Zeghlache, "Challenges for cloud networking security", In Mobile Networks and Management, Springer Berlin Heidelberg, **(2011)**, pp. 298-313.
[2] A. Iftikhar, B. A. Azween and S. A. Abdullah, "Application of Artificial neural Network in Detection of DoS attacks", SIN'09, **(2009)** October 6-10.
[3] J. Trostle, "Protecting against distributed denial of service (DDoS) attacks using distributed filtering", In Securecomm and Workshops, **(2006)** August, pp. 1-11.
[4] M. Bhaskaran, A. M. Natrarajan and S. N. Sivanandam, "Trace Backing the Spoofed IP Packets in Multi ISP Domains with Secured Communication", IEEE-ICSCN, **(2007)**, pp. 579-584.
[5] J. Kataria, P. S. Dhekne and S. Sanyal, "A Scheme to Control Flooding of Fake Route Requests in Ad-hoc Networks", In International Conference on Computers and Devices for Communications, CODEC-06, **(2006)** December.
[6] S. Sanyal, R. Bhadauria and C. Ghosh, "Secure communication in cognitive radio networks. In Computers and Devices for Communication", CODEC 4th International Conference on IEEE, **(2009)** December, pp. 1-4.
[7] D. P. Agrawal1, H. Deng, R. Poosarla and S. Sanyal, "Secure Mobile Computing", Distributed Computing –IWDC, Springer Berlin/ Heidelberg, **(2003)**, pp. 265-278.
[8] R. Bhadauria, R. Chaki, N. Chaki and S. Sanyal, "A Survey on Security Issues in Cloud Computin", arxiv.org, arXiv: 1204.0764, **(2012)**.

[9] M. Le, A. Stavrou and B. B. Kang, "Doubleguard: Detecting intrusions in multitier web applications", Dependable and Secure Computing, IEEE Transactions on, vol. 9, no. 4, **(2012)**, pp. 512-525.
[10] S. Sanyal and M. R. Thakur, "A Hybrid Approach towards Intrusion Detection Based on Artificial Immune System and Soft Computing", arXiv preprint arXiv:1205.4457, **(2012)**.
[11] M. R. Thakur and S. Sanyal, "A Multi-Dimensional approach towards Intrusion Detection System", arXiv preprint arXiv:1205.2340, **(2012)**.
[12] M. R. Thakur and S. Sanyal, "A PAXOS based State Machine Replication System for Anomaly Detection", arXiv preprint arXiv:1206.2307, **(2012)**.
[13] A. K. Trivedi, R. Kapoor, R. Arora, S. Sanyal and S. Sanyal, "RISM--Reputation Based Intrusion Detection System for Mobile Ad hoc Networks", arXiv preprint arXiv:1307.7833, **(2013)**.
[14] S. Chavan, "Adaptive neuro-fuzzy intrusion detection systems", Information Technology: Coding and Computing, Proceedings ITCC International Conference on IEEE, vol. 1, **(2004)**.
[15] A. K. Talukder and M. Chaitanya, "Architecting secure software systems", CRC Press, **(2008)**.
[16] A. Jacob, M. Paprzycki, M. Ganzha and S. Sanyal, "Applying SIMD approach to whole genome comparison on commodity hardware", In Parallel Processing and Applied Mathematics, Springer Berlin Heidelberg, **(2008)**, pp. 1220-1229.
[17] A. Ramani, S. Vhora and S. Sanyal, "The next generation Internet protocol", INFORMATICA-LJUBLJANA-, vol. 26, no. 1, **(2002)**, pp. 27-46.
[18] S. Dey, A. Abraham, B. Bandyopadhyay and S. Sanyal, "Data Hiding Techniques Using Prime and Natural Numbers", arXiv preprint arXiv:1003.3672, **(2010)**.
[19] S. Sanyal, R. A. Vasudevan, A. Abraham and M. Paprzycki, "Grid Security and Integration with Minimal Performance Degradation", arXiv preprint arXiv:1111.4545, **(2011)**.
[20] S. Sanyal, D. Gada, R. Gogri, P. Rathod, Z. Dedhia and N. Mody, "Security scheme for distributed DoS in mobile ad hoc networks", arXiv preprint arXiv:1005.0109, **(2010)**.
[21] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", InINFOCOM, Proceedings IEEE, **(2010)** March, pp. 1-9.
[22] C. H. Lin, C. Y. Lee and T. W. Wu, "A cloud-aided RSA signature scheme for sealing and storing the digital evidences in computer forensics", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 241-244.
[23] S. G. Yang, "Cloud computing security issues and mechanisms", Advanced Materials Research, vol. 225, **(2011)**, pp. 706-709.
[24] S. Dey, H. Al-Qaheri and S. Sanyal, "Embedding Secret Data in Html Web Page", arXiv preprint arXiv:1004.0459, **(2010)**.
[25] S. Sanyal, A. Tiwari and S. Sanyal, "A multifactor secure authentication system for wireless payment", In Emergent Web Intelligence: Advanced Information Retrieval, Springer London, **(2010)** pp. 341-369.
[26] V. Goyal, V. Kumar, M. Singh, A. Abraham and S. Sanyal, "CompChall: addressing password guessing attacks", In Information Technology: Coding and Computing, ITCC, International Conference on IEEE, vol. 1, **(2005)** April, pp. 739-744.
[27] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward secure and dependable storage services in cloud computing", Services Computing, IEEE Transactions on, vol. 5, no. 2, **(2012)**, pp. 220-232.
[28] V. Goyal, S. Sanyal and D. P. Agrawal, "Vcache: Caching dynamic documents", arXiv preprint arXiv:1003.2616, **(2010)**.
[29] M. R. Thakur, D. R. Khilnani, K. Gupta, S. Jain, V. Agarwal, S. Sane and P. S. Dhekne, "Detection and Prevention of Botnets and malware in an enterprise network", International Journal of Wireless and Mobile Computing, vol. 5, no. 2, **(2012)**, pp. 144-153.

Authors

Asish Aich, he is currently pursuing M.tech in Computer Science and Engineering at KIIT University, Bhubaneswar. He had also completed his MCA degree from KIIT University in 2013. His current research interest is in cloud computing, grid computing, and MCDM.

Alo Sen, she is currently pursuing M.tech in Computer Science and Engineering at KIIT University, Bhubaneswar. She had also completed her MCA degree from KIIT University in 2013. Her current research interest includes cloud computing, grid computing.