International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.2, June 2012, pp. 46~53
ISSN: 2089-3337

A Novel Open Security Framework for Cloud Computing

Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh
Cyber Law and Information Security Division
Indian Institute of Information Technology Allahabad, Uttar Pradesh-211012, India

Article Info

Article history:

Received Apr 24th, 2012
Revised May 17th, 2012
Accepted June 01th, 2012

Keyword:

Cloud Service Provider (CSP)
Virtual Image
Cloud Computing
Service Level Agreements
Identity and Access Management
Third Party Assessment

ABSTRACT

The evolution of cloud computing enables organizations to reduce their expenditure on IT infrastructure and is advantageous to both the serving and served organizations. But security issue is major concern in adoption of cloud. This paper focuses on the problem of lack of security considerations in Service Level Agreements and top security threats and vulnerability which are suggested by security experts. The Security framework for end to end security in cloud computing has also been proposed in the present work. This paper also draws attention on need of Open Security Framework. Proposed framework is developed by collective participation of security experts, practitioners, Cloud Service Providers and Clients. It is in line with various government policies, legislation and standards like ISO 27000 series, SOX, HIPPA, COBIT, ITIL etc. to comply with them. This step will boost mutual trust and privacy of participants.

Corresponding Author:

Devki Gaurav Pal,
Cyber Law and Information Security Division,
Indian Institute of Information Technology Allahabad,
Deoghat, Jhalwa, Allahabad, Uttar Pradesh-211012, India.
Email: gaurav.pal.88@gmail.com

1. INTRODUCTION

In traditional time companies used to manage their resources on their own and hesitate to disclose their data to others. Later on they started realizing management of data as over burden and reason of extra cost. To overcome this burden, they moved towards outsourcing in which they initially started giving their hardware resources to get managed by third party service providers and later they gave all their resources including data to these service providers. Thus the concept of cloud computing evolved in which companies started using these cloud servers to store, manage and even process (compute) data. Cloud computing is a scalable, fast, flexible, and cost effective technology platform for IT enabled services over the internet. Although cloud computing provide many advantages but ultimately we have to put our data on third party servers which are not directly controlled by the data owner. So security of data is the major concern in cloud computing.

To overcome this lacuna Service Level Agreements (SLA's) were made which are accepted by both the parties (service providers and consumers), but these legal agreements vary from organization to organization. These heterogeneous SLAs produced a lot of confusion regarding terms and conditions of services, cost and security features.

So these SLA's are more oriented towards service provider's benefit. Thus SLA's are not able to maintain the homogeneity as regards to Cloud Security. Figure 1 is from a survey conducted by Deloitte and CIOnet [1] to find out the reasons that are preventing organizations from adoption of Cloud Computing. Fig 1 shows that 95 % of surveyed organizations are using cloud infrastructure or planning to use in future. They are benefitting in terms of higher flexibility, cost reduction, accelerated deployment, better functionality or capability than with existing solutions. Organizations that have not yet adopted and those who have adopted cloud computing are worried for insufficient data security and risk of data availability, open compliance and legal issues. The risk of losing governance or control over data is creating doubt in the long term availability and security of data over the cloud. Adopted organizations are also worried for the same problems.

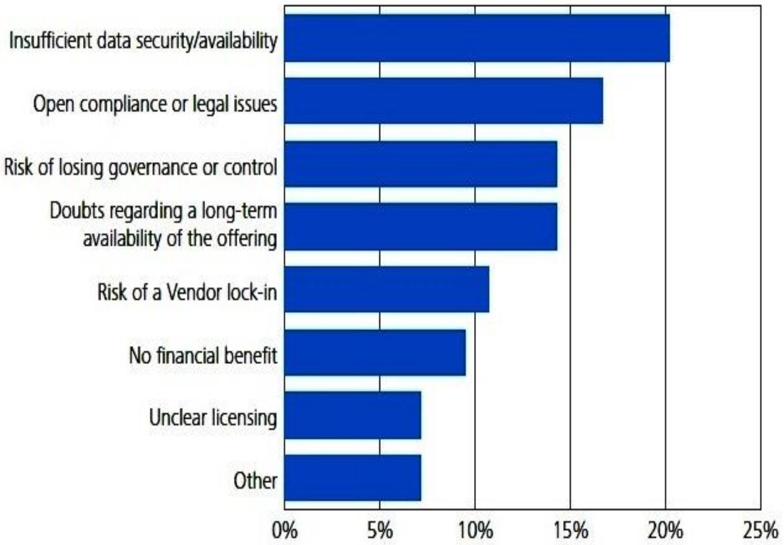

Fig 1: Cloud Adoption Survey
(*Source: Cloud Adaption Survey 2011*)

2. BACKGROUND STUDY

The big organizations like Rackspace, Amazon, Google, Microsoft, IBM, and VMware are providing cloud computing services such as data storage, an application development platform, data access and computation. They provide the complete infrastructure to manage the IT services on-demand self-basis. Customers can dynamically choose their computing services according to their changing need at reduced costs. The providers gain benefits by reusing computing resources. Thus cloud computing is advantageous to both the service providers and the clients.

Cloud computing comprises three basic service models [2]:

- Software as a Service (SaaS): This service model facilitates different types of applications provided by service provider on a cloud environment. Clients are able to access these applications with the help of interfaces like web browsers or application interfaces. Cloud application services or "Software as a Service (SaaS)" provide the function of software as a service over internet. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration setting for the application.

- Platform as a Service (PaaS): This service model provides the ability to the customer to deploy their application at the cloud environment with the use of programming and there is no need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the some configuration settings for the application where it is going to host. It also provides all the facility without the purchasing, managing and other cost of software and hardware.

- Infrastructure as a Service (IaaS): This service provides the whole infrastructure to customer for processing, networking, storing and other computing services in which the customer can run various software as well as operating systems or application based software. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except selection of the some network component like host firewalls.

Thus, cloud computing is advantageous to the enterprise and cost effective with the help of SaaS, PaaS and IaaS. However, one of the biggest problems in adoption of cloud is the lack of security. So to fulfil this security gap SecaaS has been introduced in the cloud computing.

- Security as a Service (SecaaS): The service model provides the management of security services across the internet but can provide some specialized information security service. The customer does not need to manage or handle the cloud environment like storage, servers, network, operating system, any other application except the selection of security services. By using this service the customer can access different set of services to address security. [3]

Cloud infrastructure can also be portioned into different categories on basis of their deployment methods and scope of usage. The main deployment models for cloud infrastructure are [2].

- Private Cloud: Private cloud (or internal cloud) is dedicated to the single organization comprising multiple customers and not shared with any other organizations. It is managed within the organization data centre and operated by internal employees.

- Public Cloud: Public Cloud (or external cloud) is open to use by multiple customer in the common environment. Public cloud is managed and operated by other organizations where the data will be shared among many organizations like academic, government, business organization or others.

- Hybrid Cloud: A hybrid cloud environment is the combination of different internal (private) or/and external (public) cloud providers. With the hybrid cloud, the organizations run their sensitive applications in a private cloud while the normal applications in a public cloud.

3. RELATED WORK

Wang, Ren and Lou et al. [4] have defined a public auditing system of data security by developing a privacy preserving auditing protocol. Through which an auditor can audit without having knowledge of user's data contents. They also proposed the batch auditing protocols through which multiple auditing tasks of different users are performed concurrently by TPA (Third party auditing). A public auditing system consists four algorithms (KeyGen, SigGen, GenProof, VerifyProof). KeyGen is run by the user to set up the system. SigGen is used to generate verification metadata. GenProof is executed by Cloud Server to provide a proof of data storage correctness. VerifyProof is run by TPA to audit the proof from Cloud Server.

In order to maintain cloud security, some specific methods has been proposed by Minrui Jia [5]. The author proposed solutions such as encrypt stored file, encrypt email through email solutions like offered by Hushmail, it automatically encrypt all message transmitted and received. The author had also depicted the rational use of filters Vontu, Wedsense and Vericept and other companies have proposed a system designed to monitor your network from the data, thereby automatically block sensitive data. The author also discuss the individuals privacy by addressing under some circumstances data must be shared because there is some other issues like law enforcement in which information may be compromised. The given solution well addresses the issue of stored data and the transmitted services like email to encrypt the message by some cryptographic mechanism and privacy but it should done through some standard method which is universally accepted framework.

To prevent the cloud from the intruders Sang-Ho Na, Jun-Young Park, Eui-Nam Huh [6] had proposed a framework to secure the personal cloud. They defined some cloud security threats and domain to provide better security in the personal cloud architecture. Apart from this they proposed some categories or requirements for the cloud security framework like cloud security framework has to be service based and to use non-discretionary model, single sign on and so on. The proposed system includes access control process for providing scalable service on each component such as client, end-user service portal, service configuration, service gateway, security control and monitoring. In this paper, they analyzed security threats to figure out the requirement for secure cloud infrastructure.

Alok and Abhinav et al. [7] focused on the security challenges in cloud computing. They discussed to adopt proactive approach to protect data against compromise. They discussed many security techniques like firewall, IDS, IPS, log inspection, monitoring, malware protection for line of defense, SSL, TLS and VPN for channel level security and proposed secure cloud architecture.

The proposed architecture addresses few security technologies but to secure cloud environment completely much more issues should be considered and entertained and security should be partitioned into many domains. Fedramp [11] and CSA initiatives [12]: Fedramp (Federal Risk and Authorization Management Program) is a project initiative by US government with NIST to provide a standardized approach for authorization, security assessment and continuous monitoring of cloud products and services and to enhance third party assessment. This approach uses a "do once, use many times" framework that will save cost, time, efforts, resources and staff required to conduct redundant agency security assessments. Cloud Security Alliance (CSA) [12] is also engaged in developing new frameworks and working on projects in the field of Cloud Security. The projects include 'Trusted Cloud Initiative'

(TCI), ‘Cloud Controls Matrix’ (CCM), ‘Cloud Audit’, ‘GRC Stack’, etc. These projects aim on providing global namespace, toolkit and interface from which the Assurance, Assessment, Assertion, Audit of their IaaS, PaaS and SaaS and environment’s automation is provided by the CSPs. It also provides facility to customer to operate their services with the help of secure, open and extensible way.

4. FINDINGS AND MOTIVATION TOWARDS OPEN SECURITY FRAMEWORK FOR CLOUD COMPUTING

The following findings are the views of experts from different domains of information security on latest security issues in cloud computing and its possible effective solutions:

1. The CSP’s are focusing on their own security but not of client’s security. The companies running services on the cloud make sure that their security is not compromised and they take their jobs seriously. The problem is that the focus of their security is themselves, not for the clients they serve. If an employee of one of those companies is compromised or if a client/user is misusing the system, the security parameters get foggy.
   Several of these cloud hosting services have been hacked, and if we read the fine print on the agreements, all their employees have full access to your data on their servers. (It is their server after all.)

2. At the current time, it’s hard to evaluate Cloud security. One problem is that there is no real set of standards to measure cloud security. The U.S. government just issued an initiative to develop cloud security standards called FEDRAMP. However, like most standards, it is unclear whether commercial CSP such as Google, Microsoft, Amazon and others will adopt and adhere to these standards.

3. Government pressure on service provider: If a Service Cloud is located in a country that puts secret pressure on accessing corporate files that may compromise Intellectual Property or Financial transactions.

4. Encryption key should be known to Client only: Service Providers provide the encryption service with shared key known to client and CSP. Thus any server side employee can access the client’s data. Key management should be done by Clients only or any third party service providers.

5. Security policies are not disclosed: Another issue is commercial, CSPs are very cautious about sharing security-related information with their customers and the general public. Thus clients are not aware of security policies of CSPs.

6. Certification and rating should be given to CSPs: Certification programs should be there for CSPs so that client is able to judge the CSPs according to their needs. If a CSP is not fulfilling the needs of client, client may move to other service providers.

7. External auditing should be allowed: One way to get a benchmark and insight into the security of a provider's network is to find a provider who allows external party's assessments. These external assessments should be conducted with frequency that can give confidence to the clients. If you don’t have audit results and assurances that the client wants, or if provider doesn’t allow such audits or have an assessment framework that client doesn’t approve, he may go for other best options.

8. SLA enhancements: Security information, certifications and external assessment reports should be included in SLA. SLA should address following questions like- what kind of security CSP is going to provide, what CSP would manage itself and up to what level client is allowed to manage their security themselves, how CSP will handle breaches and malicious activities and handling of screening for administrator who accesses client’s data.

9. Periodically awareness programs should be conducted for both CSP and Client employees. CSP’s employees should be technologically updated, so that they can improve security by latest trends and if any change has done, client’s employee should be informed. Client’s employee should also be trained to adopt new changes and maintain security.

Security is major concern in the cloud computing because cloud is repository of data and moving data to a common location is more attractive to attackers and more people are affected if an attack is successful. The concern for security becomes more critical when the data is managed by third party service providers. As security issues and policies are not disclosed by CSPs to their clients at satisfactory level, clients are not aware of what security services

CSPs are going to provide them. So to enhance the trust and confidence level of clients there should be an Open Security Framework managed by security experts and it should be addressed in SLA. This standard will provide a platform for complete security and external assessments.

5. PROPOSED FRAMEWORK

The security cannot be achieved at single stage, so our framework consists of eight domains which can be further divided into sub domains. All these domains should comply with various regulations and government policies like SOX, FISMA, HIPPA, COBIT, ISO/IEC 27001/2, etc. accordingly. Fig. 2 shows our proposed framework for cloud security.

1. *Physical Security*
   This domain addresses the security of physical assets like data centers, servers, storage devices, power supply, network devices and other components which help in smooth functioning of cloud services. The assets can be protected by different controls e.g. - installing CCTV equipments, biometric devices, maintaining access control registers.

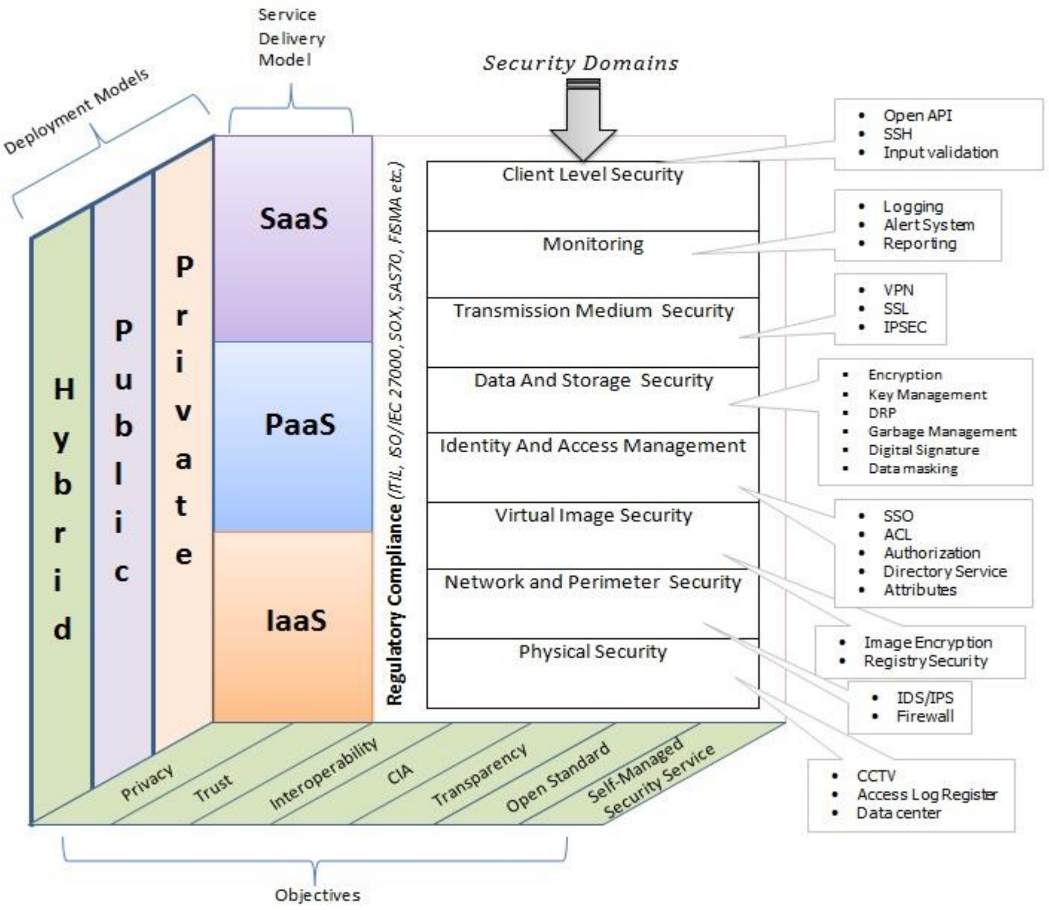

Fig 2: Proposed Cloud Security Framework for end-to-end security

2. *Network and Perimeter Security*
   This domain talks about the logical security of routers, switches, other devices and locations where the data or virtual images are stored in the data centre by configuring effectively. To achieve this security different controls e.g. - firewalls, IDS/IPS can be placed to manage security of the network by denying unauthorised access. We can deploy the AAA (Authentication, Authorization and Accountability) servers for strong authentication.

3. *Virtual Image Security*
   This domain discusses the security and integrity of the virtual images. As virtual images contain user data, so it should be considered as critical assets and security should be provided to safeguard these virtual images. All the images are created on server and an attacker or malicious code can exploit these images. Cloud provides

opportunity for attackers that they can create malicious images, in which they can execute malicious code on the same platform where the other client's images exist (common platform and resources for attackers and victims). The images can also be tampered by internal employees of service provider as they have direct access to all the images and also by internal employees of client who work on those images. To sort out this problem, encryption of virtual images, blind authentication protocol [8], provenance tracking and access control [9] have been proposed. Image name itself should be encrypted in image registry which provides linking pointer between image name and physical location.

4. *Identity and Access Management (IAM)*
IAM improves operational efficiency, regulatory compliance management by managing AAA services. Few experts suggested IAM as a Service (IDaaS) [10] to be a new service model to achieve greater security and privacy goals in cloud computing. To make it really effective redundant identity management, provisioning of cloud services, privilege management should be automated. It provides convenience to retrieve, manage, update and query for any information. It should ensure that the users have reliable, fast, cost effective access of resources and information retrieval is in a secure manner. There should be automatic identity provisioning at the time when a new customer is going to avail the services. Automated provisioning, authentication and authorization are the major concern for security. We can solve this problem by using various solutions such as single sign-on, federated identity, access control list, directory based service, access on the basis of attributes.

5. *Data Security and Storage Security*
This domain explains security of data stored on servers i.e. from data generation to usage and after usage, proper disposal of data. The data should be enough intelligent such that if it is disclosed by any unauthorized entity it should be meaningless. The goal can be achieved by using strong encryption and data masking techniques, good key management program and to maintain the integrity, digital signature technique can be opted. The proper backup service should be given to clients so that users can backup their online data and in case of any disaster they can restore their data. A reliable replication scheme and efficient file system should be opted. When the client's objective is met or the client wants to discontinue the service, client's data should be removed from server. There should be proper disposal mechanism to dispose the data because that data may contain critical information and may cause risk if reached to wrong person. A special attention must be on the garbage disposal from the virtual image location.

6. *Transmission*
This domain looks in to the question: what if data is secured in servers and at client side, but get leaked or tampered in between before the delivery at either side, i.e. security of data while transmission. In the recent days we can find a lot of incidences in which data is breached in between by man in the middle (MITM) attack or other similar attacks. We can deploy any preventive techniques available, to ensure security of data during transmission. We can choose one or combination of many techniques as per need and feasibility from VPN, SSL/TLS, IPSEC, etc.

7. *Monitoring*
This domain talks about maintaining logs and keeping checks that could be used for auditing and helps in investigation of any failure. This can be achieved by end-to-end monitoring, server and network monitoring, transaction monitoring, application monitoring, event log monitoring, etc. There should be proper automated log generation and management system to record all these types of monitoring. These logs should be reviewed and analysed periodically by an expert or some automated tools to generate reports for higher management and number of security breaches, etc. should be mentioned in these reports. An alarm system should be implemented when any anomaly is detected.

8. *Client Level Security*
This domain talks about various security techniques that must be applied at the client side to protect from various attacks like SQL injection, XSS, broken authentication, etc. [13]. Use of proprietary based APIs should be minimized and open standard based APIs or browser should be used to access cloud data. Each input from user should be validated and verified before submitting to the server.

6. CONCLUSION AND FUTURE WORK

Cloud computing has many advantages and is well adopted, but the security issue of cloud still have a big question mark. It is very difficult to manage confidentiality, integrity and availability of data in cloud. Different

CSPs are trying their best but they have their own security policies and these different policies overwhelmed the clients because they all have different set of standards and client is not aware of what and how CSPs are providing security. So a systematic and standard approach is needed. We are proposing an open framework for cloud security that can be used as a standard and we tried to cover every domain of security. Inclusion of this kind of open standard for cloud security in SLA will definitely be beneficial in terms of building trust and maintaining privacy by giving a wide range of security solutions and transparency in service policies. Thus CSPs and clients both will be benefited and they have to choose appropriate security technique according to their needs.

As our current work is in very early stage and in future it can be expanded as a complete cloud security framework by any standardizing organization. The framework should be developed by experts with involvement of CSPs and clients at every stage. Many other domains may be possibly come out like Hypervisor level security, Host Operating System level security, etc. A guideline to secure cloud from various threats and vulnerabilities may also be included. Finally, we can say cloud security is not at its maturity level and this initiative will definitely act as ray of hope.

REFERENCES

[1] “Cloud Adoption Study” Link: *http:// blog.cionet.com/wp-content/uploads/2011/10/Cloud-Adoption-Survey-2011.pdf* [Feb 6 2012].

[2] P. Mell and T. Grace, “The NIST Definition of Cloud Computing” Link: *http:// csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf* [Dec. 18 2011].

[3] M. Carvalho (2011, Oct.), “SECaaS - Security as a Service”,*Information Systems Security Association*, pp 20-24.

[4] C. Wang, Q. Wang, K. Ren and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing”, *2010 Proceedings IEEE INFOCOM*, 14-19 March, California, pp 1-9.

[5] M. Jia, "Cloud Security of Cloud Computing Application", Control*, 2011 International Conference on* Control*, Automation and Systems Engineering (CASE),* 30-31 July, Singapore, pp 1-4.

[6] S. Na, J. Park and E. Huh, "Personal Cloud Computing Security Framework", *2010 IEEE Asia-Pacific Services Computing Conference (APSCC)* , 6-10 Dec., Hangzhou , pp 671-675.

[7] A. Tripathi and A. Mishra, “Cloud Computing Security Considerations”, *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 14-16 Sept., Xi’an-Chaina, pp 1-5.

[8] Ravikiran, Shanthi and Aghila (2011, Apr.) “Securing Virtual Images Using Blind Authentication Protocol”, *International Journal of Engineering Science and Technology (IJEST),* Vol. 3 No. 4, pp 2857-2864.

[9] J. Wei, X. Zhang, G. Ammons, V. Bala and P. Ning, “Managing Security of Virtual Machine Images in a Cloud Environment”, *Proceedings of the 2009 ACM workshop on Cloud computing security*, 13 Nov, Chicago, pp 91-96.

[10] Tim, Subra, Shahed, Cloud Security and Privacy, 1st ed., United States: O'Reilly Media, 2009.

[11] “FedRAMP”, Link: *http:/ /www.gsa.gov/portal/category/10237* [Feb 12 2012].

[12] “Cloud Security Alliance”, Link: *https:// cloudsecurityalliance.org/research* [Feb 18 2012].

[13] OWASP Top 10 Security Risk”, Link: *https:// www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf* [Jan 22 2012].

BIBLIOGRAPHY OF AUTHORS

Devki Gaurav Pal completed his graduation in 2009 is pursuing his masters in cyber law and information security at Indian Institute of Information Technology, Allahabad. His research interest includes cloud computing and XML database.
Email: gaurav.pal.88@gmail.com

Ravi Krishna completed his graduation in 2009 at Uttar Pradesh Technical University and is pursuing his masters in cyber law and information security at Indian Institute of Information Technology, Allahabad. His research interest includes cloud computing, network security and cyber forensic.
Email: krishnagla@gmail.com

Prashant Srivastava completed his graduation in 2008 from Allahabad Agricultural Institute Deemed University and is pursuing his masters in cyber law and information security at Indian Institute of Information Technology, Allahabad. His research interest includes web application security, network security and database security.
Email: prashants.iiita@gmail.com

Sushil Kumar completed his graduation in 2010 at Uttar Pradesh Technical University and is pursuing his masters in cyber law and information security at Indian Institute of Information Technology, Allahabad. His research interest includes information security and network security.
Email: talk4msushil@gmail.com

Monark Bag is a Lecturer in MBA (IT) and MS (CLIS) Division of Indian Institute of Information Technology, Allahabad. He holds a B.Tech (Computer Science and Engineering), MBA (Information Technology Management) and PhD (Engineering). He is highly engaged in teaching and research. His research interest includes expert system, control chart pattern recognition, quality control, optimization techniques and intrusion detection systems. He has published many papers in reputed journals, conferences and book chapters.
Email: monarkbag@gmail.com

Vrijendra Singh is an Assistant Professor in MBA (IT) and MS (CLIS) Division of Indian Institute of Information Technology, Allahabad. He holds PhD (Independent Component Analysis and Blind Source Separation applications to Signal Processing and Artificial Neural Networks). His research interest includes information security & forensics, artificial neural networks, data mining and digital signal processing. He has published many papers in reputed journals, conferences and book chapters.
Email: vrijendra.singh@gmail.com