ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 4, September 2014

Enhancing Security and Reliability using Constraint based Information Sharing in Cloud

P.Pavan Kumar[1] , A.Ganesh[2]

[1]Assistant Professor, Department of IT, SV College of Engineering, Tirupati, Andhra Pradesh, India

[2] Assistant Professor, Department of CSE, SV College of Engineering, Tirupati, Andhra Pradesh, India

ABSTRACT: As the advancement in Information Technology grows rapidly, the term security is also one of the major concerns nowadays. The opponents sometimes may misuse the technology to steal the information. To formulate the users to interact and share data easily and immaculately with security across myriad networks, we require an environment that ensures secured and trusted information sharing. In this paper we are introducing a secure protocol for data sharing and to achieve data integrity, authentication and confidentiality using private and public cryptography and Secure Hash Algorithm (SHA-1). This protocol ensures the secure communication between the users by the use of constraint and reliability parameter of the communication nodes those involved in the interaction. Here we consider a scenario that involves customer, service contributor and the government department. This is also one of the proposed approaches for the cloud security.

KEYWORDS: Reliability Parameter, Constraint, Cloud, Encryption, Decryption.

1. INTRODUCTION

Trust and security are key enablers of the information society [2]. To make the transaction secure and reliable, trust will play a significant role. The security can be provided by using encryption techniques and also various authentication schemes are used.

To achieve the reliability of the information, the security can be provided at all individual levels for the better results. By performing various protection tasks at each level such as different techniques, we can ensure the Security. Hence the attackers or the opponents can be restricted at each level. So that the security issue can be managed as level by level approach. The security issue can be predictable by projecting it onto a [3] three-level hierarchy such as: Management level, System level, and Application and Data level. The major elements of data security involve integrity, privacy, availability, authentication which has to be taken into consideration at diverse levels within the hierarchy

There are some systems like Intelligence systems that aid international collaborations among government agencies tackle many research challenges in replicating information across agencies and organizations, interoperating transparently across heterogeneous data networks, and sharing multilingual data [5].

In our proposed approach, we have considered three nodes as customer, service contributor and government department. The customer is the person who needs a service from the service contributor and the service contributor is an organization that provides a particular service to the customer who satisfies its constraint. The government department contains both the customer and the service contributor information. To know the accuracy of the customer's information, the service contributor will communicate with government department. To maintain the security for the customer's information the government department should check the reliability parameter of that service contributor and then transfer the customer details to the service contributor.

Because, the government department shouldn't give the details of the customer to any unauthorized person or organization. The reliability parameter contains the rate of the service contributor and based on that rate the government department can reveal the customer's information to the service contributor. To make the details of the customer secured, all the information about the customer cannot be given to all contributors. After receiving the details from the government department, the service contributor checks those details of the customer with its constraint to provide the service to the customer. If the customer details are not satisfied with the constraint of the service contributor, the customer will not get any service from that service contributor. All the data transactions amid the three nodes are done using secure communication protocols. Similarly, the above scenario is also applicable for the data transmission between Cloud providers and the Cloud Users. A cloud computing provider or cloud computing service provider owns and operates cloud computing systems serve someone else. Cloud computing is being driven by providers including Google, Amazon.com, and Yahoo! as well as traditional vendors including IBM, Intel, Microsoft. A user is a consumer of cloud computing. The privacy of users in cloud computing has become of increasing concern. Let us consider a cloud i.e., Google docs. Google Drive is a file storage and synchronization service provided by Google, released on April 24, 2012, which enables user cloud storage, file sharing and collaborative editing. Google Drive is the home of Google Docs, an office suite of productivity applications, which offer collaborative editing on documents, spreadsheets, presentations, and more. Google Drive is Google's "software as a service" office suite. Documents, spreadsheets, presentations can be created with Google Drive, imported through the web interface, or sent via email. Google Docs is one of many cloud computing document-sharing services. The majority of document-sharing services require user fees, whereas Google Docs is free.[1]

In a cloud environment, data security issues and national interests mean that on-line document storage (e.g. electronic mail), and processing (e.g. Gmail) can be unsuitable for use by governments or commercial organizations, especially where sensitive data (e.g. electronic mail) or confidential data is being stored, edited or shared on systems and infrastructure that are outsourced (e.g. by senior US government officials to Google) and shared with many other organizations, individuals, users (e.g. the Internet). The proposed protocol will improve the security of the data transmission done with google docs.

II. RELATED WORKS: A SHORT REVIEW

The Literature presents a lot of works for secure communication in diverse applications. Any Information that is either minor or major has to be shared in a secure environment. Otherwise there is no information sharing. Here, we review some of the works presented in the literature.

In [9] they used the trusted computing and PEI models but they fail to use a standard protocol for encryption and decryption. In [6] they have used the trusted computing technology for the content sharing between collaborating organizations but they had not used a standard protocol for encryption and decryption. In [7] they have proposed a temporal model for group-centric secure information sharing but they had not used a standard protocol for encryption and decryption. In [4] they had not used the constraint and trust based information sharing. If we merge the standard protocol for encryption and decryption and the constraint and trust based information sharing, the information sharing will be more secured. The aforementioned information sharing techniques are used in different scenarios; among those techniques the Md. Headayetullah et al. technique [5] is comparable with our technique. Because their technique requires information from the government department and our technique requires service from the service contributor based on constraint and reliability parameter. In their technique, the security personnel need the information from the government department and the data sharing between them is through a master control. In our technique, customer need service from the service contributor and the service contributor checks the customer's information from the government department. So the information sharing in both the techniques are based on three nodes.

III. PROPOSED CONSTRAINT AND RELIABILITY BASED INFORMATION EXCHANGE

Government must keep in trust the critical asset, essential information and manage it effectively. A greater priority must be given by government organizations at all levels for the exchange of information and data between its trusted partners.

Now consider a scenario of a service contributor whom service is telephone service entity and a person (customer) entity. In this scenario, a person requests / approaches to service contributor for a service, by submitting his personal details and service requirement details, to fulfill the customer's request, the service contributor has to verify the information of customers identity and his/her provided information for fulfilling the service contributor's approval constraint. Service contributor verifies customer's information at various government departments and private bodies (here we discuss only Government bodies). The verification bodies reveal the customer's information to service contributor, so that no designated person from the service contributor can get customer's information. The information exchange shouldn't cause to any security issues and problems hence it ensures confidentiality and authentication.

This section describes the proposed technique of information sharing based on constraint and reliability parameter discussed below. Here we discuss the information sharing between the nodes customer (C) and the service contributor (SC) and a government department (GD) and vice versa. The information sharing between each node should be secured. So it is the duty of the each node to transmit the request in an unintelligible possibly encrypted manner such that the hackers cannot extract any valuable information or alter the information in the request.

Our proposed approach works as follows: A customer send request to the service contributor. Here we consider service contributor such as BSNL, the request sent by the customer is for telephone service. The service contributor i.e., the BSNL agent checks the customer's proof-id and then sends the same to Government department. Then the government department should check the reliability parameter of the service contributor and information of the customer in its database. Based on the reliability parameter of the service contributor the government department provides the details about the customer to the service contributor. The service contributor should provide the service to the customer after satisfying its constraint.

In the on hand approach, the reliability of information shared is based on the reliability parameter of the service contributor. The presented secure information sharing approach requires the following: (i) the public keys of the customer, service contributor and government departments. (ii) The government department uses reliability parameter to reveal customer details to service contributor and the constraint is needed for service contributor to provide service to customer.

<u>Reliability Parameter(RP):</u>

Definition: *"It is nothing but a measure or a parameter that is used to verify the information of a certain organization using its identity and decides whether it is a reliable organization to share the information about a customer"*.

The government department analyzes different factors related to characterize the reliability of the service contributor and also a service load balancing strategy is followed to attain good service quality.

Government department initially verifies the service contributor's registration id SC_{Rid} and if it exists in their reliability parameter list, it then checks the rate of that service contributor which is given by the customers. The reliability parameter contains the details of the service contributor. If the rate is equal to or above the target value, then the government department checks the customer details and gives the encrypted details of the customer to the service contributor based on the rate. If the rate of the service contributor is below the target value, the government department would give less details depends on the rate value. The process in the government department side after decrypting the encrypted data that is received from the service contributor is shown as below

$$checks = \begin{cases} yes, & if\ SC_{Rid} = RPD_i ; where\ i = 1,2,3,\ldots.. \\ no, & else \end{cases} . rate = \begin{cases} all, & if\ RPD_i \geq 3.5 \\ \lim ited, & else \end{cases}$$

$$customer details = \begin{cases} grant, & if\ Cp_{id} = Ad_i \\ wrongproof, & else \end{cases}$$

Where details → Details of the customer

Ad_i → Documents in the database that contains the information about customers

<u>Constraint:</u>

Definition: *"Here constraint means the terms and conditions of a certain organization that should tolerate by the customers to get the benefit from that organization or it is just like an agreement used for getting the service"*.

Each and every customer who needs a particular service from a particular organization must have to satisfy its constraint. After satisfying the constraint that customer is eligible to get the service.

3.1 Set of Operations to be performed at the Customer side:

3.1.1. Structuring the customer’s query:

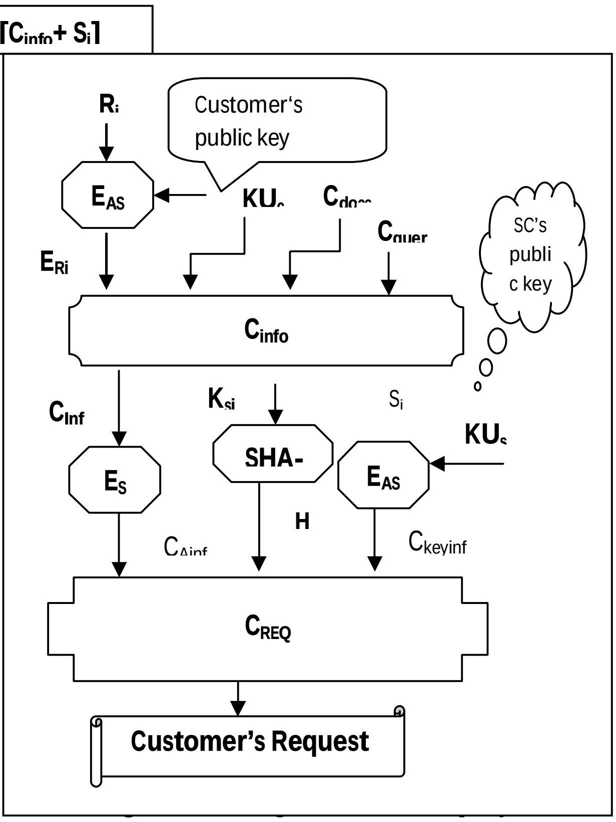
1. Encryption with customer public key KU_c
2. $\boxed{E_{Ri} \longleftarrow E_{KUc}\ [R_i]}$

Where **E** Encryption. →

R_i Request number C_{docs} → = {**d1**, d2, d3, d4,……}

3. H_i $\boxed{C_{Info} \longleftarrow E_{Ri} + Cid + C_{docs} + C_{query}}$

$\boxed{H_i \longleftarrow SHA1[C_{info} + S_i]}$



3. $\boxed{CA_{Info} \longleftarrow E_{Ksi}[\ H_i\ +\ C_{Info}\ ]}$

4. $\boxed{C_{keyData} \longleftarrow E_{KUSC}[Ks_i + S_i]}$

5.

$$\boxed{C_{REQ} \longleftarrow CA_{Info} + C_{KeyInfo}}$$

3.2. Stepladder at the service contributor:

3.2.1: Validation of the Customer's request by the Service Contributor:

i)

$$\boxed{\begin{array}{l} C_{\ REQ} \longleftarrow CA_{Info} + C_{keyInfo} \\ CAinfo \longleftarrow E_{Ks}[H_i + C_{Info}] \text{ and} \end{array}}$$

$$\boxed{Dec\ [C_{KeyInfo}]\ KR_{SC} \longleftarrow Ks_i + S_i}$$

ii)

$$\boxed{H_i` \longleftarrow SHA1\ [C_{Info} + S_i]}$$

3.2.2. The steps involved when structuring the SC's request is as follows:

1.

$$\boxed{E_{Rj} \longleftarrow Enc\ KU_{SC}\ [R_j]}$$

2.

$$\boxed{SC_{Info} \longleftarrow E_{R2} + CP_{id} + SC_{query} + SCR_{id}}$$

3. Here SHA-1 algorithm is used to maintain the data integrity.

$$\boxed{H_j \longleftarrow SHA1[SC_{Info} + S_j]}$$

4.

$$\boxed{SCA_{Info} \longleftarrow E_{Ksj}[H_j + SC_{Info}\ ]}$$

5.

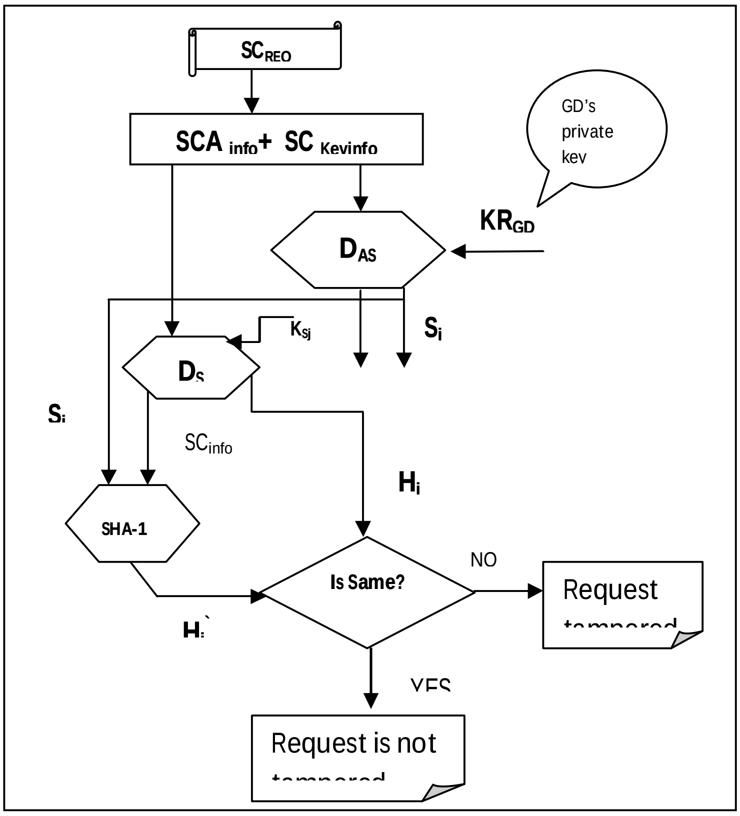
$$\boxed{SC_{KeyInfo} \longleftarrow E_{\ KUgd}\ [\ Ks_j + S_j]}$$

6. Then $SC_{keyInfo}$ and SCA_{Info} are combined to obtain SC's request SC_{REQ}.

$$\boxed{SC_{REQ} \longleftarrow SCA_{Info} + SC_{KeyInfo}}$$

3.3. Processing the SC's Request at the Government Department (GD):

3.3.1 Validation of the SC's request by Government Department:



1. The *SC's request* SCREQ is as

$$\boxed{SC_{REQ} \longleftarrow SCA_{info} + SCGD_{Keyinfo}}$$

Where, $SCA_{Info} = E_{KSj}[H_j + SC_{Info}]$ and $SCGD_{KeyInfo} = E_{KUgd}[KS_j + S_j]$

$$\boxed{Dec[SCGD_{Keyinfo}]_{KRsc} \longleftarrow KS_j + S_j}$$

If both are same, SC's request message is not tampered, otherwise tampered.

3.3.2 Structuring the GD's response: The customer's information is given by GD as response to SC's request. And also the GD has to transmit the response in a garbled possibly encrypted manner such that no hacker can access any valuable information or modify any information in the request.

1.GD's response information, $GD_{Resinfo}$ is combined with secrete value S_k and hashed with SHA-1 to obtain H_k.

2.The hash value H_k and response message $GD_{Resinfo}$ are combined, and the result is encrypted with session key KS_k to obtain $GDA_{Resinfo}$.So GD's response message $GD_{Resinfo}$ will be authenticated and confidential.

$$\boxed{GDA_{Resinfo} \leftarrow E_{KSk}[\ H_k\ +\ GD_{Resinfo}\ ]}$$

3.4. Operations performed by Service Contributor (SC) are the following:

3.4.1. Validation of GD's Response by SC:

The steps involved in the above process are as follows:

```
1.    The received response $SC_{RREQ}$ consists of $GDA_{ResInfo}$ and $GD_{ResKeyInfo}$ .
        $\mathbf{Dec[GD_{ResKeyInfo}]_{KRsc} \longrightarrow KS_k + S_k}$
        $\mathbf{Dec[GDA_{ResInfo}]_{Ks}\ \ GD_{Resinfo} \rightarrow + H_k}$
2.$H_l \longleftarrow SHA1\ [\ GD_{ResInfo}\ +\ S_k\ ]$
If $H_k == H_k^{`}$ then
Information is **not** tampered
 Endif.
```

3.4.2 Structuring the SC's response involves the following steps:

After verifying the authentication and integrity of GD's response, SC prepares and sends the response message for appropriate customer's request based upon its constraint.

$$\boxed{H_l \longleftarrow SHA1[\ SC_{Resinfo} + S_l]}$$

$$\boxed{SCA_{Resinfo} \longleftarrow E_{KSl}\ [\ H_l + SC_{Resinfo}\ ]}$$

$$\boxed{SC_{Reskeyinfo} \longleftarrow E_{KUc}[\ KS_l\ +\ S_l]}$$

$$\boxed{SC_{RESreq} \longleftarrow SCA_{info}\ +\ SC_{ResKeyinfo}}$$

The structured SC's response SC_{RESREQ} contains the $\mathbf{SCA_{ResInfo}}$ and $\mathbf{SC_{ResKeyInfo}}$.

3.5 Steps in the proposed approach at customer side:

3.5.1. Validation of SC's Response by Customer:

```
1.The received SC's response $SC_{RESREQ}$ consists of $SCA_{ResInfo}$ and $SC_{ResKeyInfo}$
        $\mathbf{Dec[SC_{ResKeyInfo}]_{KRc} \longrightarrow KS_l + S_l}$
      $\mathbf{Dec[SCA_{ResInfo}]_{Ksl} \longrightarrow GD_{Resinfo} + H_l}$

2. $H_l = SHA1[SC_{ResInfo}, S_l]$
        If $H_l == H_l^{`}$ then
    Not a tampered information
        End if
3. IF $R_i = Dec[E_{Ri}]_{KRc}$ then
                The response is valid
                End if
```

IV. RESULT AND DISCUSSION

This section details the information we used to structure the database of the government department for checking the reliability parameter of the service contributor and for checking the details of the customer and the results we obtained for our proposed constraint and trust based information sharing using that database.

Cid	SCRi d	Trustfactor	constraint	Limit of data
12456	4567	2.4	satisfied	Minimum
23458	5432	3.6	satisfied	Maximum
45678	3468	3.5	not satisfied	None
73245	7698	3	satisfied	Average

Tab:1 Result of experimentation

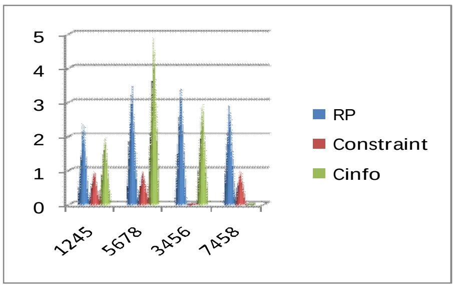
In this section, we have presented the experimental results of the constraint and trust based secure protocol in information systems. The results obtained from experiments illustrates that the presented protocol is effective secure information sharing between service contributors and government departments. The process started with a request for confidential information about customers by making use of private and public key cryptography. The government department after a security check responds with the appropriate information based on the reliability parameter with telephone service. The customer information sent will be a subset of information available with the target on the basis of the reliability parameter. At the service contributor, the legitimacy and authentication and confidentiality of the appropriate government response is verified. From the table, it is clear that the amount of information shared between service contributor and government departments depends on the reliability parameter of service provider. In this table, the field “information available in the all government departments” gives complete customer information collected from all government departments.

V. COMPARATIVE ANALYSIS

This section delineates some of the comparison between the existing technique and our technique.
The Table:2 shows the comparison of the existing technique and our proposed technique.

	Existing Approach [4]	**Proposed Approach**
Communicating Entities	3	3
Intention	To share the valuable information between security personnel &various government departments.	To transmit the vital information between service contributor and the government department.
Which hash algorithm is used ?	MD5 was used and gives less secured hash code.	SHA-1 is used and gives more secured hash code.
Encryption techniques used	Only asymmetric key algorithms were used.	Symmetric and asymmetric key algorithms.
Performance	More processing time required. More complexity.	The processing time and response time is less when we compare to existing system. Less complexity

Tab:2 Comparative Analysis



In this paper we have recommended a technique for information sharing based on ***constraint and reliability parameters***. We have used three nodes as Customer, Service Contributor and Government Department. The details about the customer and the details about the service contributor are in the database of the government department. The details of the customer would be given to the service contributor by the government department after checking the reliability parameter of the service contributor. The service contributor would provide the service to the customer after checking the constraint from customer details sent by government department. In this proposed constraint and trust based security protocol has provided authentication, confidentiality and info integrity by making use of SHA-1 Algorithm, private and public key cryptography. Because of this protocol, illegal persons cannot get the service from the service contributor and the details about the customer would be secured while transmitting customer details from customer to service contributor and government department to service contributor. We have also compared our technique with the existing technique and showed our technique is more secured than the existing technique.

REFERENCES

[1] https://docs.google.com

[2] Musau, F. ; Cheruiyot, W. ; Mushi, J.C. ; Modie, J., “Principals of Trust in Internet Security and Websecure Environment”, Computer and Management (CAMAN), 2011 International Conference.

[3] Hui-Feng Shih and Chang-Tsun Li, “Information Security Management in Digital Government”, Vol. 3, pp. 1054 - 1057, Idea Group Publishing, 2006.

[4] Violetta Cavalli-Sforza, Jaime G. Carbonell and Peter J. Jansen , “Developing Language Resources for a Transnational Digital Government System”, Language Technologies Institute, Carnegie Mellon University ,Pittsburgh, U.S.A, 2004.

[5] Md. Headayetullah, G.K. Pradhan , " Efficient and Secure Information Sharing For Security Personnels: A Role and Cooperation Based Approach ", International Journal on Computer Science and Engineering, Vol. 02, No. 04, 2010, 1254-1265.

[6] Muntaha Alawneh, Imad M. Abbadi, "Preventing information leakage between collaborating organisations",
Proceedings of the 10th international conference on Electronic commerce, Innsbruck, Austria, Article No.: 38, 2008.

[7] Peiwu Li, "A Temporal Model for Group-Centric Secure Information Sharing", Web Information Systems and Mining (WISM), 2010 International Conference on, pp. 59- 62 , 2010.

[8] Achille Fokoue, Mudhakar Srivatsa, Pankaj Rohatgi, Peter Wrobel, John Yesberg, "A decision support system for secure information sharing", Proceedings of the 14th ACM symposium on Access control models and technologies, pp:105-114, 2009.

[9] Ravi Sandhu, Kumar Ranganathan and Xinwen Zhang, " Secure Information Sharing Enabled by Trusted Computing and PEI Models", ASIACCS ’06 March 21-24, 2006, Taipei, Taiwan

[10] Peng Liu, Amit Chetal, "Trust-Based Secure Information Sharing Between Federal Government Agencies", Journal Of The American Society For Information Science And Technology—February 1, 2005.

[11] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy PreservingEHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop (CCSW “10), pp. 47-52,
2010.

[12]L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Reports by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM “10, 2010.

[14] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367-397, 2010.

[15] S. Narayan, M. Gagne´, and R. Safavi-Naini, “Privacy Preserving EHR System Using Attribute-Based Infrastructure,” Proc. ACM Cloud Computing Security Workshop.

BIOGRAPHY

First Author Mr.P.Pavan Kumar, M.Tech, working as an Assistant Professor in the Department of Information Technology, SV College of Engineering (affiliated to JNTU Anantapur), Tirupati, Andhra Pradesh, India. He received Bachelor of Technology (CSE) degree in 2010 from JNTUA, Ananthapur and Master of Technology (Computer Networks) degree in 2012 from JNTUA, Ananthapur. His research interests are Computer Networks, Network Security, and Cloud Computing.

Second Author Mr.A.Ganesh M.Tech., working as an Assistant Professor in the Department of Computer Science and Engineering, SV College of Engineering (affiliated to JNTU Anantapur), Tirupati, Andhra Pradesh, India. He received Bachelor of Technology (CSE) degree in 2008 from JNTUH, Hyderabad and Master of Technology (Computer Networks) degree in 2012 from JNTUA, Ananthapur. His research interests are Computer Networks, Network Security, and Cloud Computing.