www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 8. July 2015

SECURITY ISSUES IN CLOUD ENVIRONMENT

[1]Prof.Dr.N.Venkatesan
Associate Professor-Information Technology, Bharathiyar College of Engineering & Technology, Karaikal, India
envenki@gmail.com

[2]M.Rathan Kumar @ Prabu
HOD – Computer Engineering, ADJ Dharmambal Polytechnic College, Nagapattinam, India
rathankumarprabu@gmail.com

***Abstract*— This paper explains the security issues when a cloud user – an university, ports all its data to a cloud vendor so as to reduce the investment cost and to ensure secured data communication to and fro between the university and the cloud vendor.**

Keywords-- privacy, cloud computing, cryptography, security, intercept detection, data security

I. INTRODUCTION

This paper proposes a cloud based framework for handling the details of a University Management. Cloud Computing reduces the investment in an organization's computing infrastructure and brought up the major advancement to the IT-Industry by providing the capability to use computing and storage resources on pay as you go basis. According to market research and analysis firm IDC there is 27% rise in usage of cloud services from 2008 to 2012. All data in conventional systems is getting shifted to cloud environment. The data is huge and heterogeneous in format due to nature of the data and its dependencies. Data is to be provided in time as and when required by the users. Due importance has to be given for risk avoidance than cost saving, as threat for the data exists and data may get changed during communication across users. Hence, security becomes one of the most challenging ongoing research areas in cloud computing because data owner (the university) stores its sensitive data to remote servers and also tries to access required data from remote cloud servers which is not controlled and managed by the university. This research concentrates on employing an algorithm PASA (Privacy-Aware Security Algorithm) for university management system in a cloud environment which includes the three different security schemes to achieve the objective of maximizing the data owners control in managing the privacy mechanisms or aspects that are followed during storage, processing and accessing of different Privacy categorized data. This paper will focus on a model delivery through which the cloud users can communicate in a trusted manner.

II. RELATED WORK

A few research efforts are dealt directly with the issues of secure and privacy aware data storage and accessing in cloud computing. Sunil Sanka et al [1] proposed capability based access control technique for secure data access in cloud computing. In their scheme, the combined approach of access control and cryptography is used. The modified D-H key exchange model is also presented for user to access the outsourced data efficiently and securely from CSP's infrastructure. DR. S.N. Panda, Gaurav Kumar [3] proposed an effective intercept detection algorithm for packet transmission which uses the Exclusive-OR operation based unique encryption and decryption technique. In this scheme the forensic database also keeps the track of invalid unauthorized access and malicious activities for analyzing the behaviour of intercepts and to avoid such attempts in future.
Data privacy research in cloud computing is still in its early stages. Wassim Itani et al [2] proposed privacy as a service; a set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing. PasS supports three trust levels in CSP: first is Full Trust in which CSP is fully under trusted domain of data owner. Second is compliance based trust in this the data owner trusts on CSP to store their data in encrypted form and third is No Trust where data owner is fully responsible to maintain the data privacy. Robert Gellman [8] presents the report which discuss the various risk imposed on data privacy by the adoption of cloud computing on data privacy. Pearson [9] and S. Pearson et al [10] presents various guidelines that are considered during designing of privacy aware cloud computing services. But the detailed analyses and evaluation of fully Privacy-Aware security schemes are still an open research topic in the field of cloud computing.

III. Data Security Algorithm and Assumptions

In PASA algorithm, we assume that the four parties are involved during the communication for data storage and accessing: Data owner, cloud service provider, user and trusted module. We also assume that each party is preloaded with public keys of other so that there is no need of any PKI for distribution of public keys of each other's. For large storage and computation capacity we assume the CSP as conglomeration of several service providers like Google, Amazon and Microsoft.

IV. Proposed Algorithm

This section describes the proposed algorithm PASA (**P**rivacy **A**ware **S**ecurity **A**lgorithm) for cloud environment. In which before storing and processing the data in storage pool of CSP, the data owner classified it into three categories according to their sensitivity:

- No privacy (NP): In this category the data is not sensitive and there is no need of any form of encryption. But for network security the data can be sent via SSL.
- Privacy with trusted provider (PTP): Here the cloud provider is fully trusted by data owner. Data owner provides the sensitive data to trusted provider where the cloud provider itself is responsible for encrypting the data for maintaining its confidentiality and integrity.
- Privacy with Non-Trusted Provider (PNTP): In this category the data is highly sensitive that also needs to be concealed from cloud provider. This kind of data is encrypted on data owner side and then stored at cloud service provider.

The main focus of PASA is to maximize the data owner's control in managing all aspects of privacy mechanisms required to maintain the security of sensitive data. To achieve above defined objective PASA further includes three different security schemes for each privacy categorized data (NP, PTP and PNTP) that has different privacy aspects according to the need of sensitive data. The functional flow diagrams for NP and PTP are shown in figure 1(a)- 1(b) and their pseudo codes are shown in figure 2(a)-2(b).

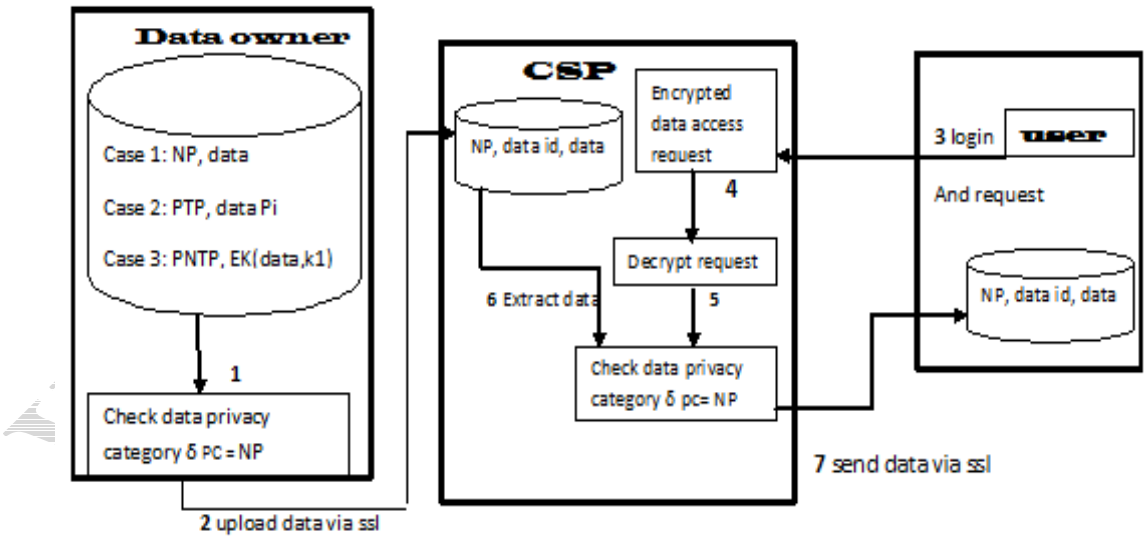

Figure 1(a) functional flow diagram of security scheme for NP category

There is no encryption and decryption of data during the storage and accessing of NP privacy category data. The user only used double encryption during the request made for accessing the data from CSP. The only requirement is that each party must be authenticated before starting their communication. Whereas in PTP security scheme the CSP is responsible to make the security of data. CSP used the X-OR operation based encryption and decryption technique which automatically generates the key without any complexity. This scheme also has unique feature of intrusion detection which prevents from various malicious activities

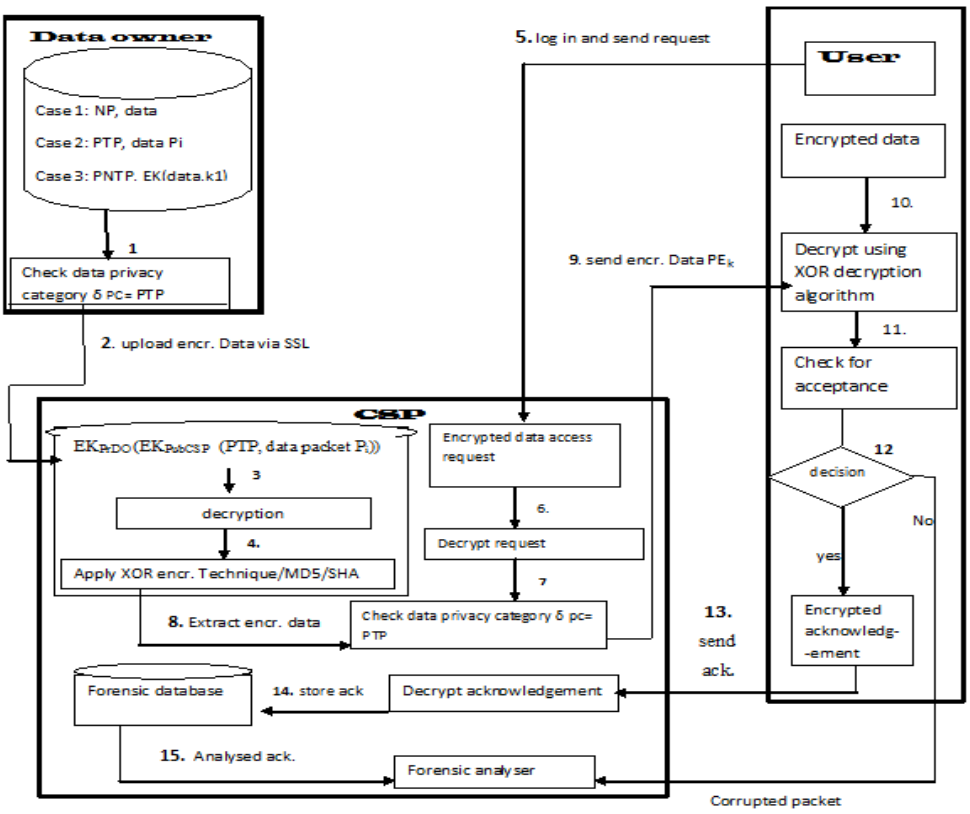

Figure 1(b) functional flow diagram of security scheme for PTP category

// Storage of NP privacy category data

Step 1: Data owner checks for data privacy category:

(a) δ_{pc} = NP // *here* δ_{pc} *represent data privacy category*

Step 2: Storage of data in storage pool of CSP:

(a) Data owner sends the data to CSP via SSL for network security where data is

δ_{DO} ⟵(NP, data id, data) // δ_{DO} *represent data send by data owner*

(b) CSP store data (δ_{DO}) in its storage pool

// secured data access between user and CSP for NP data category

Step3: User login to CSP and send request for data access

REQ $_{user}$ ⟵ EK_{PrUser} (EK_{PubCSP} (Uid, access control required, request))

Step 4: CSP check for data category and send data to user:

(a) Cloud provider receive and decrypt the request with public key of user and his own private Key

(b) check to which category requested data belong

δ_{pc} = NP //*here data Privacy category is equal to No Privacy (NP)*

(c) CSP sends the data to user via SSL for network security where data is: δ_{CSP} ⟵ (NP, data)

Step 5: End of algorithm

Figure 2 (a) Algorithm for secure storage and accessing data from CSP for NP category

// Storage of PTP privacy category data

Step 1: Data owner checks for data privacy category:

(a) δ_{pc} = PTP // *here δ_{pc} represent data privacy category*

(b) Go to step 2

Step 2: Storage of encrypted data in storage pool of CSP:

(a)Data owner send the data to CSP in encrypted form via SSL where data is:

δ_{DO} ⟵ EK_{PrDO} (EK_{PubCSP} (PTP, data packet P_i))

(b) CSP decrypt δ_{DO} and store the data in encrypted form using XOR gate based encryption technique:

1. CSP Generate a Random Key K_R by analyzing number of 1s in data PacketP_i .

(a) Develop a routine to count bits in the Data Packet

(b) Set N := Count(P_i) // Count Number of 1's in the Data Packet.

(c) Set K_R :=N // Store N in Random Number K_R

2. Apply XOR (Exclusive-OR) Operation

(a) Set EK $:= P_i \oplus K_R$

(b) The Encrypted Packet E_K is generated using XOR Operation.

(c) Set PE_K : = $\boxed{PF_i \mid E_K \mid PR_i}$ // where PF_i and PR_i has key- id and E_K Utilize as Encr.packet

3. Data Packet PE_K equipped for Transmission

// secured data access between user and CSP for PTP data category

Step3: User login to CSP and send request for data access

REQ $_{user}$ ⟵ EK_{PrUser} (EK_{PubCSP} (Uid, access control required, request))

Step 4: CSP check for data category and send data to user:

(a) Cloud provider receive and decrypt the request with public key of user and his own private Key

(b) check to which category requested data belong

δ_{Pc} = PTP //here data Privacy category is equal to Privacy with trusted provider(PTP)

(c) Go to step 5

Step5: Communication between CSP and user for accessing data of PTP category

(a) CSP send PE_K to user via SSL and user decrypt the data using following decrypting technique :

1: User Receive the Encrypted Packet PE_K

2: Check the Front PF_i and Rear End PR_i of Packet

if ($PF_i = PR_i$) Accept PFi and Set $K_R := PF_i$

Else goto Step 6

3: Generate the Binary Equivalent of K_R i.e. PB_i = Binary(K_R)

4: Perform XOR Operation i.e. $PB_i \oplus E_K$

Decryption the data E_k and get original packet P_i and Go to step 5

5: check whether the Packet is accepted or not

if (K_R = no of I's in each byte of decrypted data P_i)

Decryption Successful and Accept the Packet and user send ACK to csp

where ACK := EK_{PrUser} (EK_{PubCSP}(Uid, K_R, "successful acceptance of packet"))

CSP store ACk data to Forensic Database

Else goto step 6

6 : Insert the Record of Corrupt Packet in Forensic Database of cloud

Step 6: End of algorithm

Figure 2(b) Algorithm for secure storage and accessing data from CSP for PTP category

The functional flow diagram and pseudo code for PNTP is shown in figure 3(a)- 3(b). The PNTP privacy category data is highly sensitive data which is also concealed from CSP. For this, the data owner provides the encrypted data to CSP and the symmetric key used to encrypt and decrypt the data is sent to trusted module so that both trusted module and CSP are not able to breach the security of PNTP privacy categorized data.

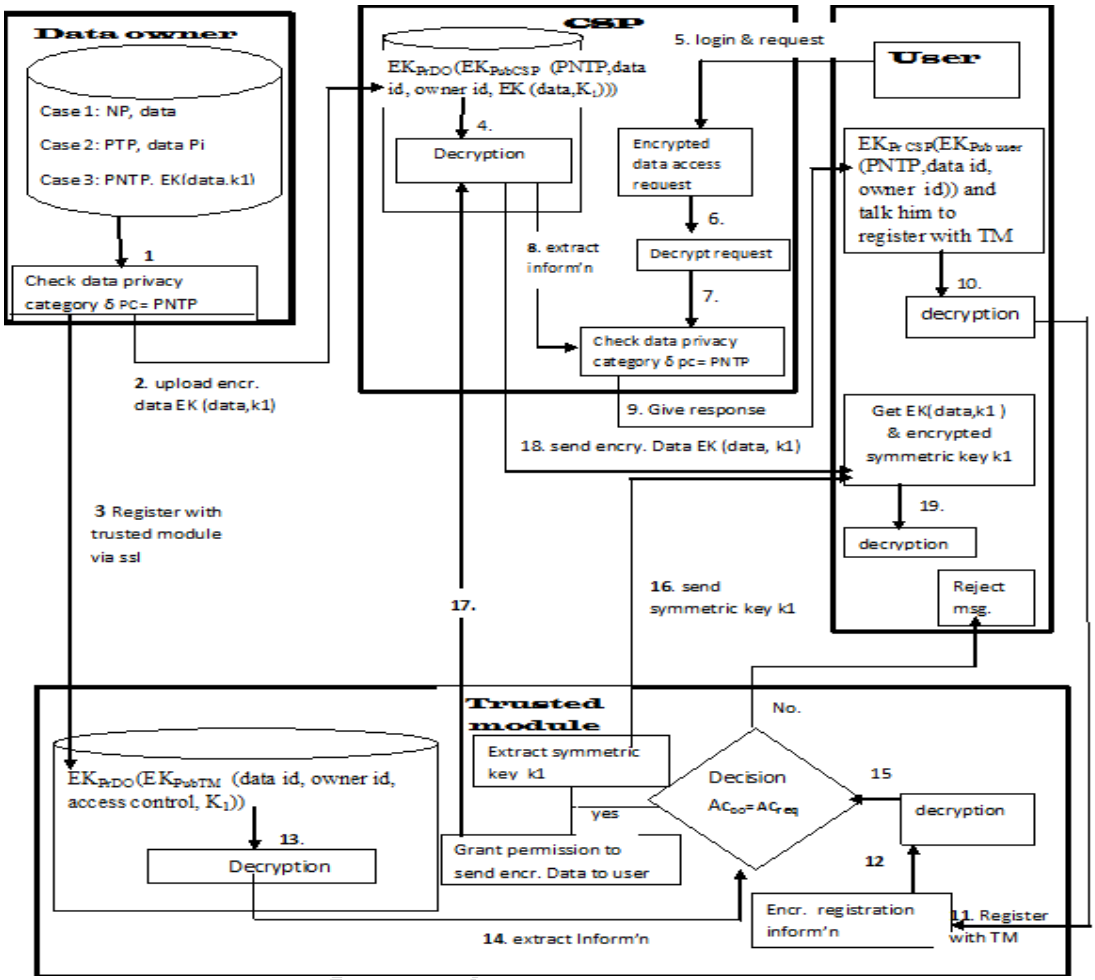

Figure 3(a) functional flow diagram of security scheme for PNTP category

// Storage of PNTP privacy category data

Step 1: Data owner checks for data privacy category:

(a) δ_{pc} = PNTP // *here δ_{pc} represent data privacy category*

(b) Go to step 2

Step 2: Data owner Store encrypted data in storage pool of CSP and register with trusted module:

(a) Data owner encrypted the data with symmetric key K_1 and send data δ_{DO} to CSP via SSL:

$\delta_{DO} \leftarrow EK_{PrDO}(EK_{PubCSP}$ (PNTP,data id, owner id, EK (data,K_1)))

(b) Data owner register with trusted module and send the following information via SSL:

$RI_{DO} \leftarrow EK_{PrDO}(EK_{PubTM}$ (PNTP, data id, owner id, access control, K_1))

(c) TM decrypts the information and get symmetric key K_1 with all other necessary Inform'n

// secured data access between user and CSP for PNTP data category

Step3: User login to CSP and send request for data access

$REQ_{user} \longleftarrow EK_{PrUser}(EK_{PubCSP}(Uid, access\ control\ required, request))$

Step 4: CSP check for data category and send data to user:

(a) Cloud provider receive and decrypt the request with public key of user and his own private Key

(b) check to which category requested data belong

δ_{pc} = PNTP *//here data Privacy category is equal to Privacy with non trusted provider (PNTP)*

(c) Go to step 5

Step 5: Communication between CSP and User for accessing data of PNTP category

(a) CSP decrypts the data δ_{DO} by public key of data owner and his own private key and get

Data $\longleftarrow$ (PNTP,data id, owner id,$EK(data,k_1)$)

(b) CSP provides δ_{CSP} to user and talk him to register with trusted module where:

$\delta_{CSP} \longleftarrow EK_{Pr\ CSP}(EK_{Pub\ user}$ (PNTP,data id, owner id))

Step6: User decrypt δ_{CSP} and register with trusted module as:

$RI_{user} \longleftarrow EK_{PrUser}(EK_{PubTM}$ (Uid, access control required, owner id, data id, PNTP))

Step7: Trusted module receive the registration information from user and check whether the Request is valid or not

(a) check $AC_{DO} = AC_{requested}$ // here the request is valid if the requested access control is equal to access control of data permitted by data owner

"Request is valid"

Go to Step 8

(b) Otherwise Go to Step 11

Step 8: Trusted module communicate with CSP and user:

(a) Trusted module sends user information to CSP as:

Send $(EK_{PrTM}(EK_{PubCSP}$ (Uid, access control, owner id, data id))) And grants permission to CSP to send the encrypted data $EK(data,k_1)$ to user

(b) Trusted module send the symmetric key K_1 to user in encrypted form i.e.

$Enc_{key} \longleftarrow EK_{Pr\ TM}(EK_{Pub\ user}$ $(K_1))$ // Enc_{key} represent encrypted symmetric key

Step9: CSP send the Encrypted data $EK(data,k_1)$ to user via SSL.

Step10: User access the original data

(a) User decrypts the Enc_{key} by using public key of Trusted Module and his own private key, and get symmetric key K_1 i.e: K_1 $DK_{pub\ TM}(DK_{pr\ user}(Enc_{key}))$

(b) By using K_1 user decrypt $EK(data,k_1)$ and get original data

(c) Otherwise

Go to step 11

Step11: Send the rejection message to user:Send ("User request can't be granted")

Step 12: End of algorithm

Figure 3(b) Algorithm for secure storage and accessing data from CSP for PNTP category

V. PERFORMANCE ANALYSIS

This section analysed the security performance and computational efficiency of proposed algorithm (PASA).

A. Security Analysis

This subsection demonstrates the robustness of proposed security algorithm towards four factors (i) Confidentiality (ii) authentication (iii) Integrity (iv) performance against attacks.

B. Data confidentiality

The proposed scheme is mainly privacy aware and data owner centric where the confidentiality is maintained according to their sensitivity and the data owner is flexible to control and manage all privacy aspects of sensitive data. This is depicted in figure 4 which is a 3-D cube chart for performance analysis of NP, PTP and PNTP. Where X, Y, Z defines security, computational efficiency and approval of packet transmission. The thickness of triangle described the level of each performance characteristics for eg. the confidentiality is considered both by PTP and PNTP but PNTP has more thick triangle and hence more confidentiality. Both PTP and PNTP also considered the Z axis which approves the packet transmission according to acceptance condition.

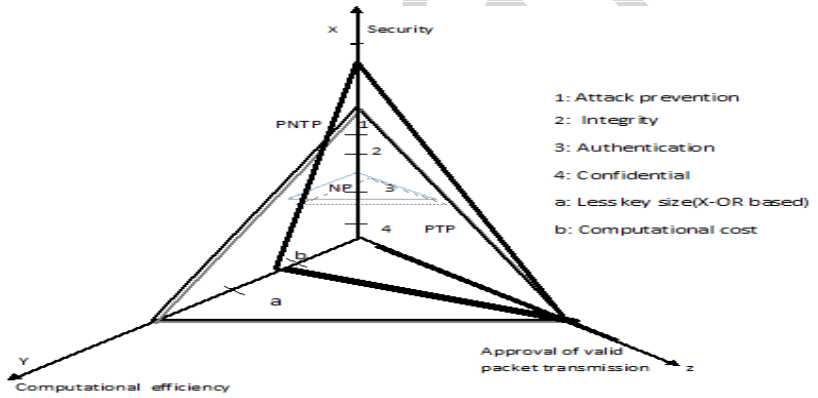

Figure 4: 3-D cube chart for performance analysis of NP, PTP and PNTP

C. Authentication

The involved parties in the proposed algorithm are authenticated by encrypting the data files every time with their own private key. In our scheme the authentication is also maintained by using SSL or login process.

D. Integrity

In the proposed algorithm (PASA) we ensures the integrity of data files by comparing the decimal form of key K_R with the number of 1's in each byte of decrypted packet. If they do not match the integrity violation is reported which is demonstrated in figure 2(b). The integrity of key is also maintained by forensic analyzer presents on server of cloud provider.

E. Performance against attacks

In PASA, double encryption scheme is used i.e. $Ek_{prsender}(Ek_{pub\ receiver}(data))$ which has longer key length and prevents from *brute force attack* because this attack become difficult on cipher. The X-OR operation based cryptography technique used for PTP in figure 2(b) behave as intrusion detection. In which the forensic analyzer analysed the various malicious activities and prevents from various types of *intrusions.* Our scheme also prevents from *man-in-the-middle* attack by using forensic analyzer because it detects the modification of data or even key. For PTP and PNTP, the CSP stores the data in encrypted form which prevents it from *inside channel attack.*

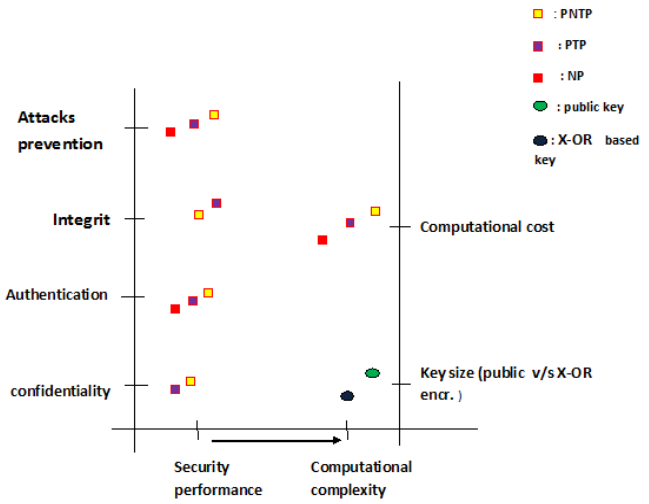

Figure 5 shows the performance characteristics for NP, PTP and PNTP Where PNTP is highly secured from attacks than PTP and NP. In this figure each category is defined by different colours and describes the level of their security performance and computational efficiency

B. computational complexity: The computational cost is increased rapidly in public key encryption when the key size increased but in proposed algorithm the X-OR operation based cryptography technique generates the key for data packet automatically without any complexity. The computational complexity of X-OR based technique as compared to public key is depicted in figure 5.

The comparison of computational cost between three security schemes i.e. for NP, PTP and PNTP is shown in table 1. Note that only dominant computation is considered i.e. encryption, decryption and authentication.

	NP	PTP	PNTP
Data owner	1 DO Auth	$1EK_{D,\ 1\ DO\ Auth}$	$2EK_{D,\ 1\ EK\ SYM}$, 2 DO Auth
CSP	$1DK_{D}$, 1 CSP Auth	$2DK_{D}$, $1EK_{x}$, 1 CSP Auth	$3DK_{D}$, $1EK_{D}$, 1 CSP Auth
USER	$1EK_{D}$, 1 user Auth	$1EK_{D}$, $1EK_{x}$	$2EK_{D}$, $2DK_{D,\ 1\ DK\ SYM}$, 2 user Auth
Trusted module	Not included	Not included	$2EK_{D}$, $2DK_{D}$

Table 1: computational cost of NP, PTP and PNTP

From this table it is clear that: Computational Cost for PNTP > Computational Cost for PTP > Computational Cost for NP where EK_D and DK_D describes the double encryption and decryption. DO Auth, User Auth and CSP Auth shows the authentication done by data owner, user and cloud provider. EKsym and DKsym describes the encryption and decryption by symmetric key, and EK_x and DK_x describes the X-OR based encryption and decryption

VI. Conclusion

This paper presented PASA (Privacy Aware Security Scheme) for cloud computing. The security solutions are mainly privacy aware and data owner centric. The paper discussed the three different privacy aware security schemes for NP, PTP and PNTP categorized data which followed the different privacy aspects according to their requirements. The paper also presented the performance analysis of proposed algorithm PASA. Future extension will: (1) consider the optimization of scheme in terms of bandwidth, memory and transmission channel consumption (2) Provide detailed evaluation of algorithm implementation.

References

[1] G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (*references*)

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73

[3]]. Sunil Sanka, chittaranjan hota, muttukrishan Rajarajan, "secure data access in cloud computing", 2010 IEEE 4th international conference on internet multimedia services architecture and application, 978-1-4244-7932-0/10 © 2010 IEEE, PP 1-6.

[4] [2]. Wassim Itani, Ayman kayssi, Ali Chehab, " Privacy as a service: privacy- aware data storage and processing in cloud computing architecture", 2009 eighth IEEE international conference on dependable autonomic and secure computing, 978-0-7695-3929-4/09 © 2009 IEEE, pp 711-717.

[5] [3]. Dr. S. N. Panda, Gaurav Kumar, ―IDATA – An Effective Intercept Detection Algorithm for Packet Transmission in Trust Architecture‖ (POT-2010-0006), selected for publication in IEEE Potentials ISSN: 0278-6648.

[6] [4]. Eoin Gleeson, "Computing industry set for a shocking change," April 2009, MoneyWeek, from http://www.moneyweek.com/investmentadvice/computing-industryset-for-a-shocking-change-43226.aspx

[7] [5]. Ajay Jangra, Renu Bala, "A Survey on various possible vulnerabilities and attacks in cloud computing environment" published in IJCBR, ISSN (Online) : 2229-6166 Volume 3 Issue 1 January 2012.

[8] [6]. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in Proc. Of ACM Cloud Computing Security Workshop 2009, pp. 55-65, 2009.

[9] [7]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. of VLDB'07, 2007.

[10] [8] Robert Gellman, "WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", February 23, 2009.

[11] [9] Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", in *Proceedings of* ICSE-*Cloud'09*, Vancouver, 2009.

[12] [10] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud", HP Labs Technical Report, HPL-2009-178,

[13] http://www.hpl.hp.com/techreports/2009/HPL-2009-178.pdf (2009)

[14] [11] W. Diffie, P.C. van Oorschot, and M.J. Wiener, "Authentication and authenticated key exchanges", Designs, Codes and Cryptography 2 (1992), 107-125.

[15] [12]. S. Kamara, and K. Lauter, "Cryptographic Cloud Storage," in Proc. Of Financial Cryptography: Workshop on real life cryptographic protocols and standardization, 2010, from

[16] http://research.microsoft.com/pubs/112576/crypto-cloud.pdf