IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 12, December 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

An Approach for Secure Sharing of Personal Health Data in Untrusted Cloud Environment

Mrs. Megha Yawalkar, Mrs. Archana Paike, Mrs. Sayali Ambavane

Department of Computer Engineering, Government Polytechnic, Pune, Maharashtra, India

ABSTRACT: The Personal Health Record (PHR) is an emerging framework of health information ex- change, which is often stored at cloud servers. But there are still various privacy problems as personal health information could be discovered to unauthorized people. To guarantee the patients control over to their own PHRs, it is a method to encrypt the PHRs before storing on cloud. But still issues such as risks of privacy, efficiency in key administration, flexible access and efficient user administration, have still remained the important challenges toward achieving better, cryptographically imposed data access control. Here in this research paper, we develop a model and mechanism for control of data access to PHRs stored in cloud servers. To achieve efficient and modular data access control for PHRs, we provide ABE encryption approach to encrypt each PHR file. In this system we try to focus on the multiple data owner scheme, and divide the users into security domains that highly reduce the key management complication for owners and users. In this system patient privacy is guaranteed by exploiting multi-authority ABE. System proposes a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the con- identicality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control.

KEYWORDS: PHR, Elgamal encryption, SHA-256, Cloud services, Revocation, RBAC

I. INTRODUCTION

Today, personal health record (PHR) has raised as a standard of health report exchange. A PHRmodel allows a user (patient) to create, manage, and control health data at one central place through the technology of web, which has thus made storing, retrieval, and sharing of the infor- mation more efficient. Here each patient is allowed to take the full control of medical records and can share health information with a variety of users, including medical report providers, family members and friends. But while it is easier to have PHR services for everyone, but there can be many security and privacy risks which could slow down its acceptance. The main rea- son to worry about is whether the patients could control the sharing of their health information (PHI), specifically when they are stored on external servers where users may not fully assur- ance. On the other side, due to the susceptible health information (PHI), the external cloud storage servers are often at risk of various attacks which may lead to vulnerability of the PHI. To ensure users (patient) confidential control on their own PHRs, it is fundamental to have fine data access control model that works with non-trusted servers.

Objectives of system

- To implement a system that can provide security and privacy of PHR file using Elgamal encryption as well as proxy re-encryption.
- To define Role base Access Control (RBAC) algorithm for access control mechanism.
- Implement a proxy revocation when any trusted user revoked by data owner.
- Re-encryption has implement using different algorithm like SHA-256 or AES 128 16 bit encryption algorithm.
- Evaluate a system performance in Amazon EC2 public cloud with trusted, semi trusted as well as un-trusted environment.

A basic idea would be to encrypt the data before storing on cloud. Here basically, the PHR owner should be able to decide how to encrypt files and to allow or not which users to retrieve access to each file. A PHR record file must only be accessible to the users who are given the decryption key, while it remains confidential to the other users. Next would be that the patient shall always have the right to not only allow, but also be able to access authorization when they feel it is necessary. However, the patient-centric privacy is often in danger with amount of scalability in a PHR system. The

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

certified users may either need to retrieve the PHR for own use or authoritative use. On the other side, different from the single data owner type which is often considered in most of the previous works, in a PHR system, there are numerous userswho may encrypt according to their own possible ways, by using different sets of cryptographic keys. Here a concern would be, allowing each user acquire keys from every owner whose PHR wants to be read would limit the access since patients are not always online. So an alternative way would be to employ a central authority to do all the key management for all PHR owners, but this again requires too much trust on an authority.

II. LITERATURE SURVEY

In [1], Hamid et al. target the confidentiality of healthcare patient's multimedia data in the cloud by proposing a tri-party one-round authenticated key agreement protocol based on bilinear pair- ing cryptography. The proposed protocol can generate a session key among the participants to communicate securely. Finally, the private healthcare data is accessed and stored securely by implementing a decoy technique with a fog computing facility. Nonetheless, the proposed ap- proach incurs a computational overhead cost in communication in sacrifice for strong security. In [2], Marwan et al. propose a novel method based on Shamirs Secret Share Scheme (SSS) and multi-cloud concept to enhance the reliability of cloud storage in order to meet security requirements to avoid loss of data, unauthorized access, and privacy disclosure. The proposed technique divides the secret data into many small shares so that one does not reveal any informa- tion about medical records. Besides, mutli-cloud architecture, data are spread across different cloud storage systems. In such a scenario, cloud consumers encrypt their data using SSS tech- nique to ensure confidentiality and privacy. Therefore, the healthcare data are split into various shares so that data confidentiality is guaranteed. On contrary, the paper does not discuss any as- pects of the optimal number of shares for the incurred trade-off between efficiency and security. It does not discuss the quality analysis of recovered healthcare data.

In [3], Galletta et al. present a system developed at Instituto di Ricovero e Cura a Carattere Scientifico (IRCCS) that is claimed to address the patient's data security and privacy. The pre- sented system is based on two software components the anonymizer and splitter. The first col- lects anonymize clinical data, whereas the second obfuscates and stores data in multiple cloud storage providers. Thus, only authorized clinical operators can access data over the Cloud. They present a case study that uses Magnetic Resonance Imaging (MRI) data to assess the per- formance of the implemented system. The paper [4] discusses important concepts related to EHRs sharing and integration in health- care clouds and analyze the arising security and privacy issues in access and management of EHRs. The paper presents several basic security and privacy requirements for application clouds: ownership, authenticity, non-repudiation, patient consent and authorization, integrity and confidentiality and availability, archiving and auditing. Then they present an EHR security reference model for managing security issues in healthcare clouds, which highlights three im- portant core components in securing an EHR cloud: secure collection and integration, secure storage and access management, and secure usage model. Finally, they illustrate the develop- ment of the proposed EHR security reference model through a use-case scenario and describe the corresponding security countermeasures and possible security techniques.

The paper [5] lists various methods of encryption and also addresses security and privacy chal- lenges in healthcare cloud by deploying a novel framework with Cloud-based Privacy aware Role Based Access Control (CPRBAC) model. The side goal is to reduce computational com- plexity and communication overhead. However, there is no qualitative analysis discussion on the efficiency of the approach and its mitigation to security and privacy attacksIn [6], Padaki et al. survey several healthcare security lapses pertaining to non-repudiation, CIA model, and what it means to stakeholders in the healthcare industry. They also discuss few proven operational strategies, risk management methodologies and discern what the indus- try can do to mitigate such security risks and privacy threats. The paper classifies the security threats posed on healthcare clouds into three high level categories including: network, system care and protection, and compliance with standard acts and rules. Ibrahim et al. [7] propose a framework which allows secure sharing of EHRs over the Cloud among different healthcare providers. In the proposed framework, Public Key Infrastructure (PKI) is used to maintain authentication between participating healthcare providers and the EHR sharing cloud. The proposed framework claims that it ensures the confidentiality, integrity, au- thenticity, availability and auditability. It also claims that it meets the security standards defined in the technical safeguards of the HIPAA Security Rule.

In general, the owner is defined as the creator of the information. Establishing information ownership is necessary for protection against unauthorized access or misuse of patient's medi- cal information. Ownership of healthcare information can be protected through a combination of encryption and watermarking techniques that results in secured healthcare information that cannot be transmitted, accessed, or released without the mutual acceptance of all entities in- volved in the ownership/creation of the healthcare information. Patients can allow or deny the sharing of their information with other healthcare practitioners [8]. To implement patient data sharing in a healthcare system, patient

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

may grant rights to users based on a role or attributes held by the respective user to share specific healthcare data with that user Authenticity in general refers to the truthfulness of origins, attributions, commitments, and in- tentions. It ensures that the entity requesting access is authentic. In healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified via the Authentication Act [9]. The authentication of information can pose special problems, like man-in-the middle attacks, and is often mitigated with a combination of usernames and passwords. Most cryptographic protocols include some form of endpoint authentication specifically to prevent man-in-the-middle attacks. In a healthcare system, both healthcare information offered by providers and identities of consumers should be verified at every access.

Confidentiality is the act of ensuring that patients health data is kept completely undisclosed to unauthorized entities. Delegating data control to the cloud, leads to an increase in the risk of data compromises, as the data becomes accessible to an augmented number of parties. Due to the increased number of parties, devices and applications involved, there is an increase in data compromise threats. To make the patient/doctor relationship work effectively, it is necessary for the patient to trust the healthcare system to protect the confidentiality of his data. If the patient feels that the information he gives to his doctor is not protected, and that his privacy is threatened, he can be more selective about the information he will provide to his doctor in the future. The threat of data compromise can harm the patient/doctor relationship and hamper the proper medical diagnosis and treatment [10]. For example, an employer may refuse a job if the patient's medical data are disclosed. Confidentiality can be achieved by access control and using encryption techniques.

Auditing is a security measure that ensures the safety of a healthcare system. Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access and modification of data. Both HIPAA and Health Information Technol- ogy for Economic and Clinical Health (HITECH) require users within the healthcare provider's organization to be held accountable for their actions when handling patients' protected health information. There are different approaches to maintaining audit controls for such information; for example, Integrating the Healthcare Enterprise (IHE) [11] specifies a profile for the Audit Trail that contains sufficient information to answer questions such as: For some user: which patient's records was accessed? For some patient's record: which users accessed it? What user authentication failures were reported? Such approaches could help administrators mitigate in- sider threats by ensuring detection of unauthorized access and illegal disclosure of healthcare records. Auditing could also help detect attempts by hackers to break into a public healthcare cloud system and help administrators detect potential vulnerabilities in the system.

Cloud computing and the widespread connectivity, have increased the risk of data breaches. Health data is highly sensitive and safeguarding this data is a high priority for individuals, healthcare providers, and cloud services providers. Encryption is considered an important part of the security policy of organizations and service providers because it can circumvent intruders gaining value from data. Encryption is a technique that is used to scramble cleartext data into ciphertext with a key. The key is used later by authorized party to decode data to the original form. Encryption uses a computer algorithm to decode data and generate the key where know- ing or guessing the key is highly difficult. Ciphertext (encrypted data) is considered more secure from the clear text data and it prevents unauthorized users from obtaining a value or meaning from accessing the data. In cloud computing, encryption must be considered during data in motion, data at storage, and during data deletion [12].

Jung, Taeho, et al.[13] "Control cloud data access privilege and anonymity with fully anony- mous attribute-based encryption." Confidentiality is the act of ensuring that patients health data is kept completely undisclosed to unauthorized entities. Delegating data control to the cloud, leads to an increase in the risk of data compromises, as the data becomes accessible to an aug- mented number of parties. Due to the increased number of parties, devices and applications involved, there is an increase in data compromise threats. To make the patient/doctor relation- ship work effectively, it is necessary for the patient to trust the healthcare system to protect the confidentiality of his data. If the patient feels that the information he gives to his doctor is not protected, and that his privacy is threatened, he can be more selective about the information he will provide to his doctor in the future. The threat of data compromise can harm the pa- tient/doctor relationship and hamper the proper medical diagnosis and treatment. For example, an employer may refuse a job if the patient's medical data are disclosed. Confidentiality can be achieved by access control and using encryption techniques.

Goh, Eu-Jin, et al.[14] "SiRiUS: Securing Remote Untrusted Storage.", a secure file system considered to be encrusted ended with insecure network and P2P file systems . SiRiUS adopts the network storing is untrusted and offers its own read-write cryptographic access control for file level sharing. Key management and user revocation is simple with minimal out-of-band communication. File system are maintained by SiRiUS using hash tree constructions. SiR- iUS

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

contains a new method of performing file random access in a crypto graphical method file without the use of a block server. Extension lead to SiRiUS includes large scale group sharing using the NNL key revocation structure. To implementation of SiRiUS makes the relative to the basic file system despite using cryptographic operations. SiRiUS contains a new method of performance file random access in a cryptographic method by file without the use of a block server. Using crypto graphical operations implementation of Sirius also possible. Private Key share the each group member must be updated but joining of new group user in the group.

Ateniese, Giuseppe, et al.[15] "Improved proxy re-encryption schemes with applications to se- cure distributed storage." proposed method of proxy re-encryptions to use the access control to the secure file system and distributed storage. The data owner encrypted the block of content with symmetric key and unique, that is encrypted all block of content under a master public key. Moreover, to contribution of a users public key, the suitable block content keys from the mas- ter public key is straight re-encrypt using proxy cryptography that helps in keeping the access control and improvement of security. To manage access to encrypted content stored on spread untrusted replicas, this method create used in centralized access control server. The main profits of this method are unidirectional and only a limited volume of trust is set in the proxy. While, a collusion attack can happen between any revoked malicious user and untrusted cloud server permit them to find out the decryption keys of all the encrypted blocks of content.

III. PROPSOED SYSTEM DESIGN

In the proposed research work to design and implement a system that can provide the security to Personnel Health Records (PHR) files using semi trusted proxy re-encryption services, and eliminate the insider attacks like collusion attack, bruited force attack as well as SQL injection attack.

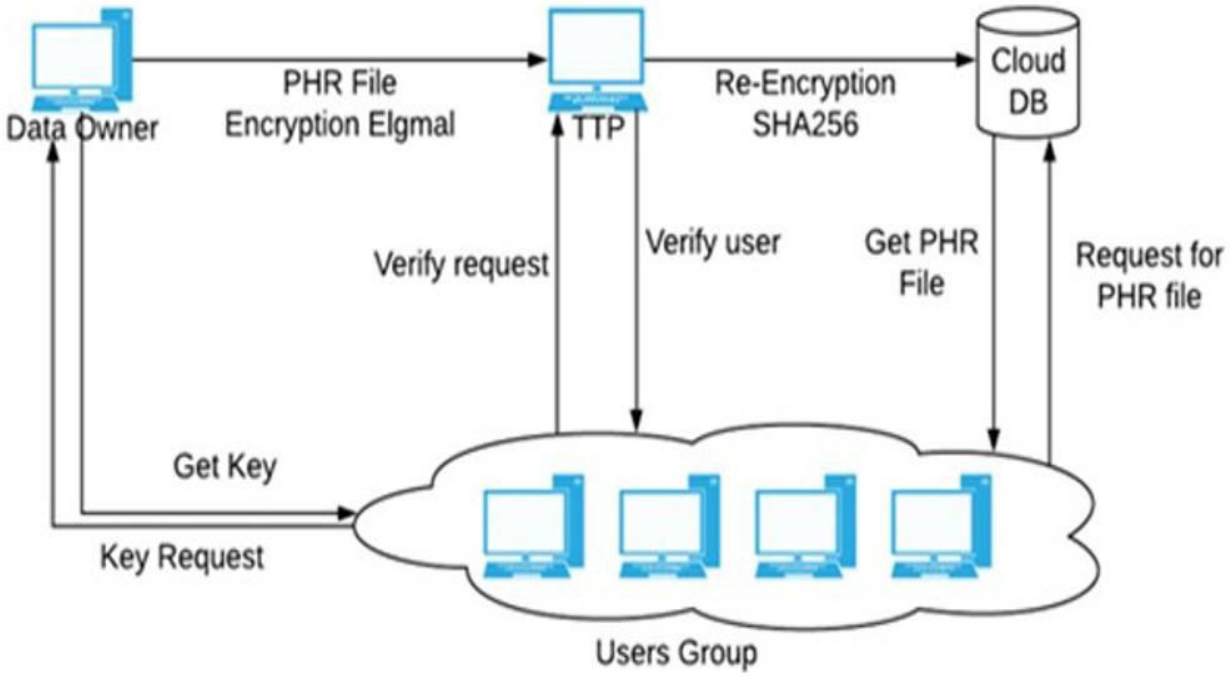

Figure 1 : Proposed system architecture

Here we perform a PHR system where there are numerous PHR owners and PHR users. The owners could be patients who have full access control over their own PHR data where they can construct/generate, maintain and delete it. There is a server which belongs to the PHR service provider which stores all the owners' PHRs. The users may come from various fields; for example say a friend, a guardian or a researcher. Here users try to access the PHR records through the server to read or write to someone's PHR, and at the same time users have right to access to multiple owners.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

IV. RESULTS AND DISCUSSIONS

According to proposed survey system provide the highest security of personnel; heath care data in cloud environment.

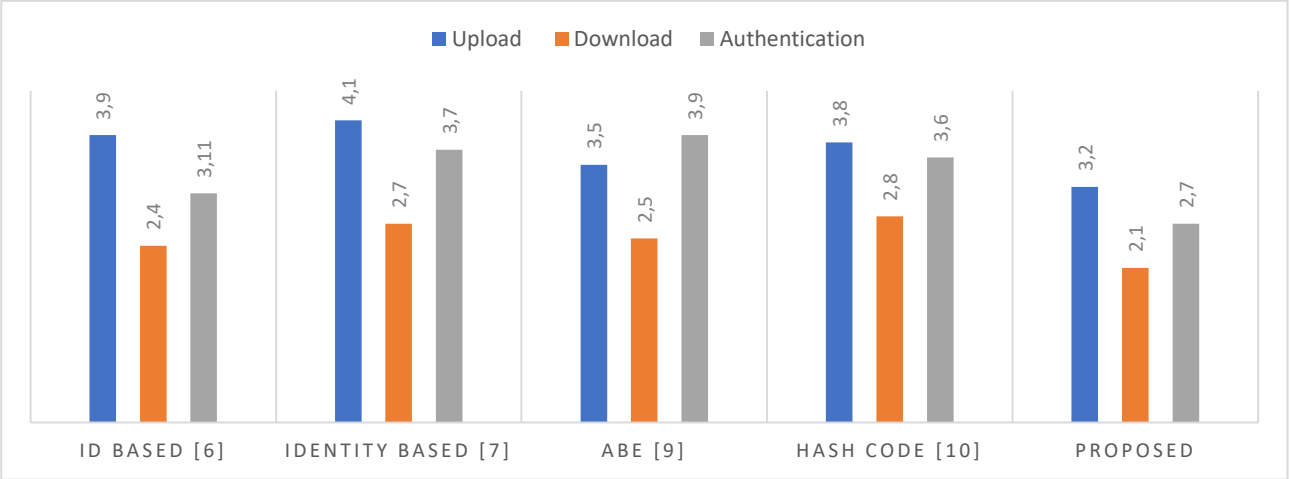

Figure 2 :System Performance Measures proposed vs Existing approaches

The system [11] and [12] denote the Attribute Base Encryption (ABE) as well cloud storage.The system used the Attribute authorities for user verification and revocation purpose.The system required multiple certificate authorities for user verification that can be take more time. In the proposed system it can remove the such dependencies using Trusted Third Party (TTP).The system has also deploy on Amazon EC2 with public cloud environment.All the table Metrics Evaluation shows the Time required in milliseconds for file data encryption and file data decryption.

Table 1 : Performance analysis of proposed system

Data size in KB	Encryption Time (Milliseconds)	Decryption Time (Milliseconds)
5	515	612
10	1025	1033
15	1547	1556

All the table Metrics Evaluation shows the Time required in milliseconds for file data encryption and file data decryption.

V. CONCLUSION

Data security is the major problem in cloud storage. Before outsourcing PHR into the third party server different attribute based encryption schemes are used for secure storage. ABE is used to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliation. Using Enhance MA ABE scheme, better on demand revocation is possible. In practical case some more problems will arise. The main issue in this case is trying to implement work flow based conditions. For solving these need attribute-based broadcast encryption (ABBE). Work flow Based situation is implement using ABBE and analyze security and computation cost. From analysis show that this work flow based scheme is both scalable and efficient. It gives better on demand user revocation also. In future it would be interesting to consider Attribute Based Broadcast Encryption system with different types of impressibility. If consider different credential are equal then Distributed ABE scheme is needed.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 12, December 2020 ||

REFERENCES

[1] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, A Secu- rity Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography, IEEE Access, 2017.
[2] M. Marwan, A. Kartit, and H. Ouahmane, Protecting medical data in cloud storage us- ingfaulttolerance mechanism, in Proceedings of the 2017 International Conference on Smart Digital Environment, 2017, pp. 214 219.
[3] A.Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti, and M. Villari, An approach to share MRI data over the Cloud preserving patients privacy, in Computers and Communications (ISCC), 2017 IEEE Symposium on, 2017, pp. 94 99.
[4] R. Zhang and L. Liu, Security models and requirements for healthcare application clouds, in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 268 275.
[5] K. Shah and V. Prasad, Security for Healthcare Data on Cloud, 2017. [6] S. Supriya and S. Padaki, Data Security and Privacy Challenges in Adopting Solutions for IOT, in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cy- ber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on, 2016, pp. 410 415.
[7] A. Ibrahim, B. Mahmood, and M. Singhal, A secure framework for sharing Electronic Health Records over Clouds, in Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on, 2016, pp. 1 8.
[8] P.Metri and G. Sarote, Privacy issues and challenges in cloud computing, Int. J. Adv. Eng. Sci. Technol., vol. 5, no. 1, pp. 5 6, 2011. An Approach for Secure Sharing of Personal Health Data in Untrusted Cloud Environment
[9] Washington Electronic Authentication Act, Revised Code of Washington, Vol RCW, vol. 70, no. 10, 1992.
[10] P.Duquenoy, N. M. Mekawie, and M. Springett, Patients, trust and ethics in informa- tion privacy in eHealth, in eHealth: Legal, Ethical and Governance Challenges, Springer, 2013, pp. 275 295.
[11] Integrating the Healthcare Enterprise, IHE Profiles. 2017.
[12] L. Coyne et al., Ibm private, public, and hybrid cloud storage solutions. IBM Redbooks, 2017.
[13]Jung, Taeho, et al. ”Control cloud data access privilege and anonymity with fully anony- mous attribute-based encryption.” IEEE transactions on information forensics and security 10.1 (2015): 190-199.
[14] Goh, Eu-Jin, et al. ”SiRiUS: Securing Remote Untrusted Storage.” NDSS. Vol. 3. 2003.
[15] Ateniese, Giuseppe, et al. ”Improved proxy re-encryption schemes with applications to secure distributed storage.” ACM Transactions on Information and System Security (TISSEC) 9.1 (2006): 1 - 30.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details