IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

A Novel Approach for Efficient Data Sharing and Revocation with Data Access control

Narsimha Banothu[1*], P. Dayaker[2], P. Bhaskara Reddy[3]

[1, 2] Department of CSE, Holy Mary Institute of Technology & Science, Keesara, Hyderabad, Telangana
[3]Department of ECE, Holy Mary Institute of Technology & Science, Keesara, Hyderabad, Telangana

Available online at: www.ijcseonline.org

Accepted: 25/Nov/2018, Published: 30/Nov/2018

Abstract: The novel paradigm of data outsourcing on the cloud is a double-edged sword. On the one hand, it frees data management owners and allows data owners to more easily share their data with targeted users. On the other hand, this poses new challenges in terms of privacy and security. In order to protect the confidentiality of data from the honest but curious cloud service provider, many works have been proposed to support data access control with precise rules. However, so far, no system is able to support both granular access control and the publication of time-sensitive data. In this article, integrating timed cryptography into Cipher text cryptographic encryption (CP-ABE) encryption, we propose a new control of time access and attributes on time-sensitive data for archiving. In the public cloud (called TAFC). Based on the proposed scheme, we also propose an efficient approach to designing policies to access the various access requirements for time-sensitive data. The in-depth analysis of safety and performance shows that the proposed scheme is highly efficient and meets the security requirements for data storage in the public cloud.

Keywords: Cloud storage, Cipher text cryptographic encryption, programmed-release encryption

I. INTROUDCTION

The cloud storage service offers significant benefits in terms of data sharing and cost reduction. As a result, more and more businesses and individuals are outsourcing their data to the cloud to benefit from this service. However, this new paradigm of data storage poses new challenges in maintaining data confidentiality. Because the cloud service separates data from the cloud service client (individuals or entities), denying them direct control over that data, the data owner cannot trust the cloud server to perform secure access control to the data. As a result, the problem of secure access control has become a difficult issue in public cloud storage. Encrypted encryption-based encryption (CP-ABE) is a cryptographic method useful for controlling data access in cloud storage. All of these CP-ABE-based systems enable data owners to gain accurate and flexible access control over their data. However, CP-ABE determines the privilege of user access only based on their intrinsic attributes, without other critical factors, such as the time factor. In fact, the time factor usually plays an important role in the management of time-sensitive data (for example, the publication of a new generation e-magazine or the exposure of the company's future business plan). In these scenarios, both the release privilege mechanism and the fine access control should be considered. For example, consider enterprise data exposures: a company typically prepares important files for the different expected users, and these users can obtain their access privileges at different times. For example, the future plan of this company could contain trade secrets. In the beginning, the access privilege can only be issued to the CEO. As a result, the managers of some relevant departments may be granted access privileges at a later date if they take responsibility for the implementation of the plan. In the end, other employees in some specific departments in the organization can access the data to assess the completeness of that business plan. When downloading time-sensitive data to the cloud, the data owner wants different users to access the content after several times. When archiving outsourced data, CP-ABE can characterize different users and provide fine access control. However, to our knowledge, these systems cannot support the gradual release of access privileges. From the point of view of cryptography, the function of releasing timed access privileges can be provided by programmed-release encryption (TRE). Rivest et al proposed this first TRE practical algorithm, which was then introduced in different scenarios. In a TRE-based system, a trusted agent, rather than a data owner, can constantly issue the access privilege at a given time. Some schemes, such as those proposed for the integration of TRE in the control of remote access to data. However, these systems lack a precise access control or leave an unbearable burden. How to achieve timely access control and precise access control in cloud storage? A simple but naive method is to manage the time factor as an attribute. However, an unsustainable number of time-related keys must be delivered to each user at any pre-established time, resulting in significant overhead for both calculation and communication. Qin et al. made a preliminary attempt to integrate time with attributes, but only addresses the question of the duration of each user's attributes. A more practical requirement is that each user with a different set of attributes may have different release time points for the same file. Unfortunately, the Qin program cannot meet this requirement[1,2].

The main contributions of this project can be summarized as follows:
1) By integrating THRE and CP-ABE into public cloud archiving, we offer an efficient system for accurate and secure access control for time-sensitive data. In the proposed scheme, the data owner can autonomously designate the intended users and their relative privilege of access by releasing time points. In addition to performing the function, it is shown that the load is negligible for the owners, the users, and the trusted CA.
2) We present how to design the access structure for any potential temporary version access policy, in particular by integrating several publication times for different users. To our knowledge, we are the first to study the structural design approach for time-sensitive data access requirements.
3) In addition, a rigorous safety test is provided to confirm that the proposed scheme is safe and effective.

II. LITERATURE SURVEY EXISTING SYSTEM

Rivest et al. an algorithm proposed by TRE which has been used in different scenarios. In a TRE-based system, a trusted agent, rather than a data owner, can constantly issue the access privilege at a given time. Some schemes have been proposed to integrate TRE in the control of remote access to data.

Qin et al. Preliminary attempt to integrate time with attributes, but only addresses the quality of life problem of each user's attributes. A more practical requirement is that each user with a different set of attributes may have different release time points for the same file. Unfortunately, the Qin program cannot meet this requirement.

Disadvantages

CP-ABE determines the access privilege of users only based on their intrinsic attributes without other critical factors, such as the time factor. These schemas do not support the gradual release of access privileges. These systems do not have precise access control or leave an unbearable burden.

III. PROPOSED SYSTEM

In this project, we propose an efficient time-based access control system and attributes, called TAFC, for time-sensitive data in the public cloud. Our scheme has two important capabilities:

1) Inherits the property of fine granularity of CP-ABE;
2) Introducing the hatch mechanism, maintain the characteristics of time release of TRE.

Note that in TAFC, the introduced trap mechanism only affects the time factor and only a corresponding secret must be published when exposing the associated traps. This makes our system very efficient, which translates into a small cost for the original system based on the CP-ABE.

We should investigate how to design an efficient access structure to construct arbitrary access privileges with time and attribute factors, especially when incorporating an access strategy to allow more access privileges.

As an extension of the previous version of the conference, we present potential sub-policies for time-sensitive data and therefore present an efficient and practical method for building relevant access structures.

Advantages

By integrating THRE and CP-ABE into public cloud storage, we provide an efficient frame work for obtaining secure, fine-grained access control for time-sensitive data[4].

In the proposed scheme, the data owner can autonomously designate the intended users and their relative privilege of access by releasing time points. In addition to performing the function, it is shown that the load is negligible for the owners, the users, and the trusted CA.

We present how to design the access structure for any potential temporary version access policy, especially by integrating multiple exit points for different users.
To our knowledge, we are the first to study the structural design approach for time-sensitive data access requirements. In addition, a rigorous safety test is provided to confirm that the proposed scheme is safe and effective.

1) Achieving secure, scalable, and fine-grained data access control in cloud computing

Cloud computing [3] is an emerging computing paradigm in which IT infrastructure resources are provided as Internet services. As promising as it may be, this paradigm also raises many new challenges in data security and access control when users outsource sensitive data to be shared on cloud servers that are not part of the same trusted domain respect to data owners. In order for sensitive data to remain confidential from unreliable servers, legacy solutions generally enforce cryptographic methods by disclosing only the decryption keys of data to authorized users.

However, in doing so, these solutions inevitably introduce a significant computational overhead for data owner for key distribution and data management when access control over fine granular data is desired, and therefore does not fit good.

The problem of simultaneity, scalability and privacy of access control data is still unresolved. This document addresses this problem by defining and applying access policies based on data attributes and allowing the data owner to delegate most of the computational activities involved in controlling access to data attributes detailed data unapproved cloud servers without disclosing the contents of the underlying data. We achieve this goal by exploiting and combining uniquely attribute-based encryption (ABE), proxy re-encryption and lazy re-encryption techniques. Our proposed scheme also presents the essential properties of the confidentiality of user access privileges and the responsibility of the secret keys of users. The in-depth analysis shows that our proposed schemes are very efficient and safe with existing security models.

2) Cipher text-policy attribute-based encryption

In many distributed systems, the user must be able to access the data only if a user has some set of credentials or attributes. Currently, the only way to implement such policies is to use a reliable server to store data and mediate access control. However, if a server that stores data is compromised, the confidentiality of the data will be compromised. In this paper, we present a system for implementing complex access control over encrypted data that we call cryptography based on the attributes of the cryptographic criterion. Using our techniques, the encrypted data can remain confidential even if the storage server is unreliable; in addition, our methods are secure against collusion attacks. Cryptographic systems based on the previous attributes used attributes to describe the encrypted data and policies created in the user's keys. While in our system, attributes are used to describe the credentials of a user and a party that encrypts the data determines a criterion for determining who can decode. As a result, our methods are conceptually closer to traditional access control methods, such as role-based access control (RBAC)[8]. In addition, we provide an implementation of our system and provide performance metrics.

3) Attribute-based access control with efficient revocation in data outsourcing systems

The application of authorization policies and the support of policy updates are among the most difficult problems to solve in the data outsourcing scenario. Encryption based on encrypted text policy[5] attributes is a promising cryptographic solution to address these issues and to enforce access control policies defined by the data owner on outsourced data. However, the problem of applying attribute-based encryption in an outsourced architecture poses several challenges in relation to the revocation of attributes and users. In this document. We propose an access control mechanism that uses cryptography based on cryptographic policy attributes to enforce access control policies with efficient user attribute and revocation features. Granular access control can be achieved with a double encryption mechanism that exploits attribute-based encryption and the distribution of selective group keys in each attribute group. We show how to apply the proposed mechanism to securely manage data outsourced. The results of the analysis indicate that the proposed scheme is efficient and safe in data outsourcing systems.

4) Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption

The Personal Health Record (PHR)[6] is a new model of patient-centered health information exchange, which is often outsourced to be stored by third parties, such as cloud service providers. However, there have been many privacy concerns as personal health information may be exposed to such third party servers and unauthorized third parties. To ensure patient control over access to their DSPs, this is a promising method for encrypting DSPs before outsourcing. However, issues such as privacy risks, scalability in key management, flexible access, and efficient user rejection remained the most important challenges in gaining granular and cryptographic access to the data. access to data. In this article, we propose a new patient-centric framework and a set of mechanisms to control access to PHR data stored on semi-traceable servers. To gain access to accurate and up-to-date PHR data, we use attribute-based encryption (ABE) techniques to encrypt PHR files for each patient. Unlike previous data outsourcing work, we focus on the multiple data owner scenario and divide users in the PHR system into multiple security domains that significantly reduce the complexity of key management for owners and users. A high degree of patient confidentiality is ensured simultaneously by exploiting the multiauthoric ABE. Our schema also allows for dynamic modification of access policies or files attributes, supports efficient on-demand user / attribute revocation and emergency access in emergency scenarios. Detailed analytical and experimental results are presented that show the security, scalability and effectiveness of our proposed scheme.

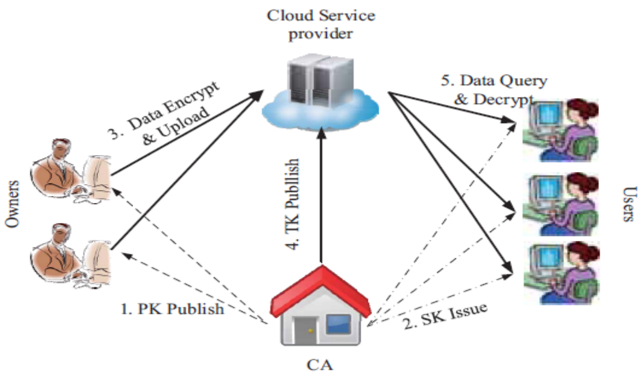
5) Key-aggregate cryptosystem for scalable data sharing in cloud storage

Data sharing is an important feature of cloud storage. In this project, we show how to share data securely, efficiently and flexibly with other users in cloud storage. We describe the

New public-key cryptosystems that produce cryptograms of consistent size so that efficient delegation of decryption rights is possible for any set of ciphers. The novelty is that it is possible to aggregate any series of secret keys and make them compact as a single key, but by understanding the power of all the aggregated keys. In other words, the secret key holder can issue a constant-sized aggregate key for flexible choices of cryptographic text defined in the cloud storage, but the other encrypted files outside the set remain reserved. This compact aggregate key can easily be sent to other people or stored on a smart card with very limited secure storage space. We provide a formal security analysis of our systems in the standard model. We also describe other applications of our systems. In particular, our systems provide the first public-controlled cryptography controlled by the patient for a flexible hierarchy, which was not yet known.

IV. DESIGN

ARCHITECTURE



V. IMPLEMENTATION

Central authority:

The central authority (CA) is capable to deal with the security assurance of the entire framework: It distributes framework parameters and conveys security keys to every client. Likewise, it goes about as a period operator to keep up the coordinated discharging function.CA is thought to be completely trusted, while clients could be malignant. CA is in charge of key dispersion and time token distributing. A malevolent client will attempt to unscramble the figure writings to acquire unapproved information by any conceivable means, incorporating intriguing with different vindictive clients.

Data Owner:

The data owner (Owner) chooses the entrance arrangement in light of a particular characteristic set and at least one discharging time focuses for each document, and afterward scrambles the record under the chose approach before transferring it. In detail, the proprietor scrambles his/her message for the reason that planned clients can decode it after an assigned time. From the security angle, TRE fulfills that: 1) Except the planned clients, nobody can get any data of the message [10]; 2) Even the proposed client can't get the plaintext of the message before the assigned discharging time.

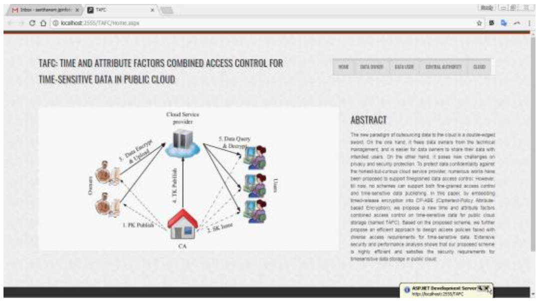
Data Consumer:

The data consumer (User) is allocated a security key from CA. He/she can question any figure content put away in the cloud, yet can decode it just if both of the accompanying requirements are fulfilled: 1) His/her property set fulfills the entrance strategy; 2) The present access time is later than the particular discharging time[9].

Cloud Service Provider:

Cloud service provider (Cloud) [7] incorporates the chairman of the cloud and cloud servers. The cloud attempts the capacity errand for different substances, and executes get to benefit discharging calculation under the control of CA. In our entrance control framework, the cloud is thought to be straightforward yet inquisitive. From one perspective, it offers solid stockpiling administration and effectively executes each calculation mission for different elements; then again, it might attempt to increase unapproved data for its own advantages.

Results

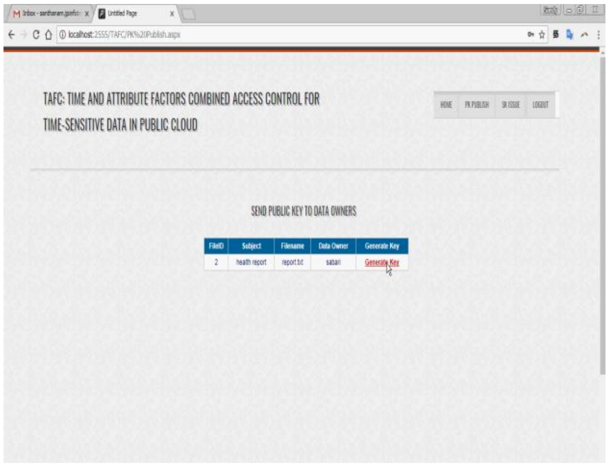


TAFC: TIME AND ATTRIBUTE FACTORS COMBINED ACCESS CONTROL FOR TIME-SENSITIVE DATA IN PUBLIC CLOUD

ABSTRACT

The new paradigm of outsourcing data to the cloud is a double-edged sword. On the one hand, it frees data owners from the technical management, and is easier for data owners to share their data with intended users. On the other hand, it poses new challenges on privacy and security protection. To protect data confidentiality against the honest-but-curious cloud service provider, numerous works have been proposed to support fine-grained data access control. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. In this paper, by embedding timed-release encryption into CP-ABE (Ciphertext-Policy Attribute-based Encryption), we propose a new time and attribute factors combined access control on time-sensitive data for public cloud storage (named TAFC). Based on the proposed scheme, we further propose an efficient approach to design access policies faced with diverse access requirements for time-sensitive data. Extensive security and performance analyses shows that our proposed scheme is highly efficient and satisfies the security requirements for timesensitive data storage in public cloud.

Fig 1: this is Home page, any user can access to navigate and register all other pages.

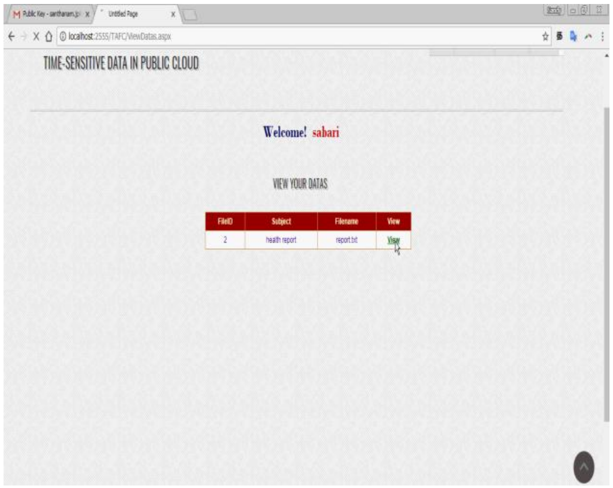


TAFC: TIME AND ATTRIBUTE FACTORS COMBINED ACCESS CONTROL FOR TIME-SENSITIVE DATA IN PUBLIC CLOUD

SEND PUBLIC KEY TO DATA OWNERS

FileID	Subject	Filename	Data Owner	Generate Key
2	health report	report.txt	sabari	Generate Key

Fig 2: In this page, generate a public key to the data owner user.



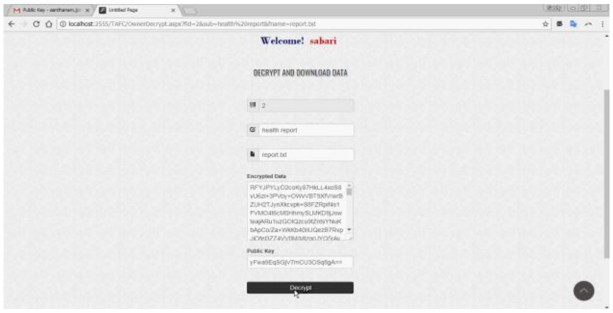
TIME-SENSITIVE DATA IN PUBLIC CLOUD

Welcome! sabari

VIEW YOUR DATAS

FileID	Subject	Filename	View
2	health report	report.txt	View

Fig 3: In this page, view the list of data files.


Public Key - santhanam.jp
Untitled Page
localhost:2555/TAFC/OwnerDecrypt.aspx?fid=2&sub=health%20report&fname=report.txt
Decrypt

Welcome! sabari

DECRYPT AND DOWNLOAD DATA

2

health report

report.txt

Encrypted Data

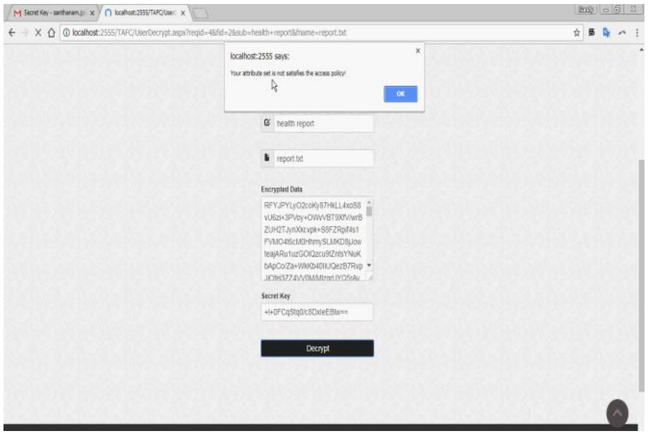
RFYJPYLyO2coKy87HkLL4xoS8
vU6zi+3PVby+OWVBT9XfV/wrB
ZUH2TJynXkcvpk+S8FZRpif4s1
FVMO4t6cM0HhmySLMKD8jJow
teajARu1uzGOIQzcu9tZntsYNuK
bApCo/Za+WkKb40IiJQezB7Rvp
JiOfrI3Z74VVBM/MtzgrUYO5rAv

Public Key

yFwa9Eq9GjV7mCU3OSq8gA==

Fig 4: in this page, data owner user is decrypting the data.

Access policy


Secret Key - santhanam.jp
localhost:2555/TAFC/User
localhost:2555/TAFC/UserDecrypt.aspx?reqid=4&fid=2&sub=health+report&fname=report.txt
OK
Decrypt

localhost:2555 says:

Your attribute set is not satisfies the access policy!

health report

report.txt

Encrypted Data

RFYJPYLyO2coKy87HkLL4xoS8
vU6zi+3PVby+OWVBT9XfV/wrB
ZUH2TJynXkcvpk+S8FZRpif4s1
FVMO4t6cM0HhmySLMKD8jJow
teajARu1uzGOIQzcu9tZntsYNuK
bApCo/Za+WkKb40IiJQezB7Rvp
JiOfrI3Z74VVBM/MtzgrUYO5rAv

Secret Key

+I+0FCqStq0/c8DxleEBlw==

Fig 5: in this page, decrypt key data neither was nor access policies.

CONCLUSION

This project goes for fine-grained get to control for time touchy information in distributed storage. One test is to all the while accomplish both adaptable planned discharge and fine granularity with lightweight overhead, which was not investigated in existing works. In this paper, we proposed a plan to accomplish this objective. Our plan consistently fuses the idea of planned discharge encryption to the design of cipher text approach quality based encryption. With a suit of proposed systems, this plan furnishes information proprietors with the capacity to adaptably discharge the entrance benefit to various clients at various time, as per a very much characterized get to arrangement over qualities and discharge time. We additionally considered access strategy outline for all potential access prerequisites of time delicate, through appropriate arrangement of time trapdoors. The examination demonstrates that our plan can safeguard the classification of time-touchy information, with a lightweight overhead on both CA and information proprietors. It hence well suits the down to earth extensive scale get to control framework for distributed storage.

REFERENCES

[1] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, “A surveyof proxy re-encryption for secure data sharing in cloudcomputing,” IEEE Transactions on Services Computing,Avaliable online, 2016.

[2] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef,“Transparent data deduplication in the cloud,” inProceedings of the 22nd ACM SIGSAC Conference onComputer and Communications Security, pp. 886–900,ACM, 2015.

[3] R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, andA. Ali, “Cloud authorization: exploring techniques and approach towards effective access control framework,”Frontiers of Computer Science, vol. 9, no. 2, pp. 297–321, 2015.

[4] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16,no. 1, pp. 69–73, 2012.

[5] J. Bethencourt, A. Sahai, and B. Waters, “Cipher text policy attribute-based encryption,” in Proceedings of the28th IEEE Symposium on Security and Privacy (S&P’07), pp. 321–334, IEEE, 2007.

[6] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754,2012.

[7] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, “DACMACS: Effective data access control for multi-authority cloud storage systems,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[8] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalableand secure sharing of personal health recordsin cloud computing using attribute-based encryption,”IEEE Transactions on Parallel and Distributed Systems,vol. 24, no. 1, pp. 131–143, 2013.

[9] E. Bertino, P. A. Bonatti, and E. Ferrari, “TRBAC: Atemporal role-based access control model,” ACM Transactionson Information and System Security, vol. 4, no. 3,pp. 191–233, 2001.

[10] I. Ray and M. Toahchoodee, “A spatio-temporal rolebasedaccess control model,” in IFIP Annual Conferenceon Data and Applications Security and Privacy, pp. 211–226, Springer, 2007.

Authors Profile

Narsimha Banothu, Associate Professor in the Department of CSE at Holy Mary Institute of Technology and Science, Hyderabad. Telangana. He has published 16 Papers in reputed international journals**,** 2 National & International conferences. He is also the Life time Member of CSI, IAENG. His Research areas are Data mining, Information Security and Cloud computing.

Dr. P. Dayaker, Associate Professor in CSE at Holy Mary Institute of Technology and Science, Hyderabad. Telangana. He has received Ph.D in Computer Science and Engineering from Acharya Nagarjuna University. He Published 24 Papers in reputed international journals, 4 National & International conferences. He is also the Life time Member of ISTE, CSTA, IAENG, IRED. He is IUCEE – IIEECP Certified Engineering Educator and BYST, INDIA – CITY & GUILDS, UK Certified Mentor. He received many awards like BEST FACULTY; BEST ORDINATOR from Here maps Solutions Pvt.Ltd. His Research areas are Wireless Sensor Network, Information Security and Internet of Things, Cloud computing Blockchain technology.

Dr. P. Bhaskara Reddy, the Director HITS is a and dynamic Professor of ECE, has 30 years of Industry, Teaching, Research and Administrative experience in Reputed Engineering Colleges & Industry. In 28 years of experience served various positions from Asst. Professor to Principal/Director Research & Guidance: Published 2 Books 1. “Information Technology in Technical Education – Economic Development by “LAMBERT Academic Publishing” 2. Innovative Methods of Teaching Electronic Devices and Circuits by “Hi Tech Publisher” Published 9 Laboratory Manuals, 126 Research papers at National and International Level journals / Conferences on Education, Electronics Communication, I.T, Computer Networks, E-Commerce etc. Guided 5 Research Scholars for their Doctorates, about 50 M.Tech., M.C.A. and B.Tech projects and completed 2 DST Projects an amount of Rs.72.83 Lakhs. Symposiums Conducted: 12 National Level Technical Symposiums on various topics in Electronics & Communications, Computers etc. Awards Received: 1). Bharath Jyothi Award in 2003 from IIFS, New Delhi, 2). Rastraprathiba Award in 2004 from ICSEP, New Delhi, 3). Knowledge Award from Alumni of SVHCE for the year 2001.