IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Efficient Signcryption with Verifiable DesigncryptionFor Sharing Personal Health Record

Chethan V[1*], Vijay Kumar N[2], Karan Deep SV[3], Pallavi[4], Jagadeesh BN[5]

[1,2,3,4,5]Dept of Computer science, East West Institute of Technology, Visvesvaraya Technological University, India

DOI: https://doi.org/10.26438/ijcse/v7si15.198202 | Available online at: www.ijcseonline.org

Abstract—PHR is a patient-centric approach of health information exchange, that allows to store, access and to share the personal health information. To share confidential resources at the optimal cost, the PHR service providers are willing to keep the health information in the cloud. Some of the private agencies can expose the health information to some unauthorized persons because patient will not be having the physical control of the PHR. So To Overcome this problem, CipherText-Policy Attribute Based Signcryption is employed for sharing the PHR. It provides a access Control, confidentiality, authenticity of the Information. But it brings a high computational overhead and low efficiency in designcryption process. so some of the major computation are given to the Ciphertext Transformed Server that leaves only a small burden to the PHR User.The system is also capable of computing some unexpected Computations. Futhermore theoretical analysis and desired security properties includes confidentiality, unforgetability and verifiability has been proved in random oracle model.

Keywords—Personal health record system, Attribute-based signcryption, Cloud computing, Outsourcing computation.

I. INTRODUCTION

In the rapid development of cloud computing, alarge number of companies and individuals utilize the public cloud to store and share data. By outsourcingdata in the cloud, the users no longer need to maintain the local storage. Taking Personal Health Record (PHR) system for example, many PHR services are outsourced to the cloudserver to enjoy the benefits of cloud computing. The users can access their PHR data from cloud rather than from the PHR service providers. Undoubtedly, the cloud-assisted PHR system attracts a lot of attention from government and industry. An unauthorized user may access or modify the PHR data stored in the cloud server. On the other hand, the PHR data collected from patients might be polluted if the malicious adversary delivers the false data to the PHR service provider. Therefore, the most crucial question is how to ensure the PHR data is only available to the users who are authorized by the PHR owner. And how to ensure the data collected from patients is authentic without disclosing the identity of the patients. Recently, Attribute-Based Encryption (ABE) [1] has gotten widespread attention in the research community. It realizes fine-grained access control and converts one-toone communication mode into one-to-many communication modes. it can effectively ensure the confidentiality of data. There are two types of ABE, named as keypolicy ABE (KP-ABE) [2] [3] and ciphertext-policy ABE (CPABE) [4] [5], respectively. In the KP-ABE scheme, attribute set is used to annotate the ciphertexts and access policies are associated with users' private keys. In the CP-ABE scheme, each ciphertext is associated with an access policy, and each user's private key is associated with attribute set. Only when the attribute set satisfies the access policy, the corresponding ciphertext can be decrypted.

In order to achieve the confidentiality and authenticity simultaneously, an efficient and flexible method named as Attribute-Based Signcryption (ABSC) [7]. Indeed, ABSC has been applied to secure cloud-assisted PHR system due to its unique characteristics. In addition, the plaintext is signcrypted and uploaded to the cloudserver in the PHR system. Then, the signcryption operation only needs to be executed once. However, the frequency of designcryption operation is far greater than signcryption operation. [8] introduced a CP-ABSC scheme for cloud-based PHR sharing system which provided fine-grained access control, confidentiality, authenticity, signcryptor privacy and public verifiability, simultaneously.

CONTRIBUTIONS

We are present a new Cipher text-Policy Attribute- Based Signcryption with Outsourced Designcryption (CPOABSC) scheme in the cloud-based PHR system. As far as we know, this is the first time to equip the secure outsourcing to the ABSC scheme.

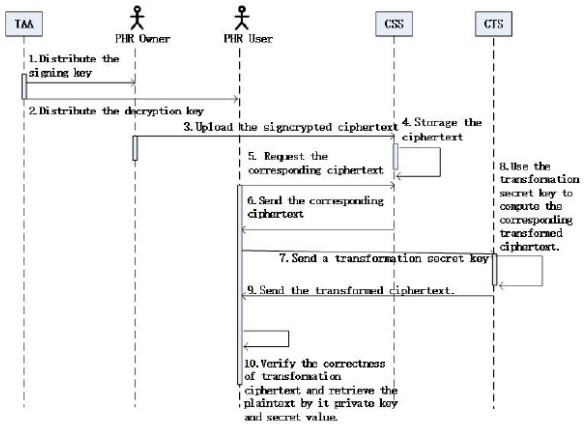

Fig. 1: High-level description of our protocol.

The main contributions are as follows:

- The verifiability for the CP-OABSC has also been modeled formally verifiable outsourcing of designcryption can be viewed as the sophisticated combination of ABE schemes with verifiable outsourcing decryption and server-aided signature verification.
- In order to reduce the expansion rate of cipher-text, we utilize a mixed signcryption technology, in which an attribute-based encryption method is used. encryption algorithm is used to encrypt the PHR data.
- Also prove the correctness and security of the proposed scheme and its complexity and efficiency are also analyzed. We further compare our scheme with other ABSC schemes in terms of signing key size, decryption key size and ciphertext size, the computational cost of signcryption and designcryption.

II. RELATED WORK

2.1 Secure Outsourcing of Attribute-Based Encryption

To reduce computational cost on the user side, Green etal. [18] proposed a decryption algorithm in which complex computation is outsourced to an untrusted third-party and left a small computational overhead for users to recover the plaintext. They utilized a semi-trusted cloud server to transform any ABE cipher text into an ElGamal-style ciphertext In addition, the semi-trusted cloud server knows nothing about the plaintext and the user's private key. In order to outsource the decryption computation to a cloud server, a user needs to use his private key to generate a blind key (*BK*) and a retrieving key (*RK*). The user transmits the *BK* to the cloud server, then the cloud server returns an ElGamal-style ciphertext to the sender. Finally, the user utilizes the *RK* to recover the plaintext. However, in their scheme, a dishonest cloud server may return a fake result by replacing the original ciphertext and its tag with another ciphertext and corresponding tag. To ensure the correctness of the transformation ciphertext returned from the semi-trusted cloud server. Lai *et al*. [9] suggested a concrete construction to verify the correctness of the transformed ciphertext. In their construction, a component which composed of a real message and a random message is introduced. However, the original untransformed ciphertext is also required to be input in the final decryption stage. Compared with [18], this method causes nearly double in both ciphertext size and decryption operation cost.

To increase the efficiency of Lai's scheme in [9], a key encapsulated mechanism (KEM) was introduced in [10] and [11],simultaneously. Their methods decrease the communication cost and computation cost nearly by half compared with Lai's scheme [9]. Similarly, the scheme in [12]encrypts a message and a random number together. The random number is used to realize verifiability. Li *et al*. [13] considered the huge computation overhead at both the attribute authority center side and user side. They presented a new outsourced ABE scheme which not only supporting outsourced decryption but also enabling delegating key generation. In their scheme, the actual attributes and a default attribute are embedded into a user's private key. The computation related to the actual attributes is outsourced to the cloud server and the computation associated with the default attribute is performed by the attribute authority center. Then, the terminal user's private key can be obtained by merging these two parts together. Moreover, the method of outsourced decryption is same as [18]. Ma *et al*. [14] proposed two ciphertext-policy attribute-based key encapsulation mechanisms (CP-AB-KEM). They are the first one to take into account the verifiable of outsourced encryption and outsourced decryption. Furthermore, their mechanisms provide exculpability, which means that the users can't accuse the Decryption Service Providers (DSP) to return incorrect results. Similarly, an outsourced ABE scheme with anti-fraud function was proposed by Xu*et al*. [19]. Their scheme prevents the cloud server from deceiving the users.The encrypted data can't be transformed without the permit even they meet the access conditions actually. Taking into account the overall efficiency of the system, Zhang *et al*. [20] and Wang *et al*. [21] presented the schemes which not only achieved secure outsourced key-issuing, encryption

And decryption, but also increased the communication cost at the client side.Recently, with the development of outsourced ABE, most of researchers have drawn attention to deploy the outsourced ABE technology to reduce the computational cost and communication overhead on user side and authority side. For example, Li *et al*. [22] applied the outsourced key generation and outsourced decryption to an ABE system which holds the keyword search function. In [23], Li *et al*. achieved a highly efficient user revocation by outsourcing both of the computation of encryption and

decryption to cloud servers. In [24], Li *et al*. combined the verifiable outsourced decryption technique with the ABE scheme which possesses the property of constant ciphertext length. In [25], Wang *et al.* achieved user's anonymity and multiauthority efficiently through the introduction of outsourcing decryption technology.

2.2 Attribute-Based Signature

Fuzzy identity-based signature (IBS) was presented and formalized in [26] [27] which allows a user to sign with part of his attributes. In addition, the verifier can check whether the signature is signed or not. In order to obtain the same purpose as IBS, the concept of ABS was presented in [28]. However, neither of these types of signatures takethe anonymity of the signer into consideration. Considering the anonymity of the signer, Maji*et al*. proposed an ABS scheme in [6] which based on groups with bilinear pairings and knew the privacy of the signer. Their construction supports predicate which described by monotone span programs. However, it only proved to be secure in the generic group model. For the purpose of constructing an efficient ABS scheme with provable security under a standard hardness assumption, Shahandashti and Safavi- Naini [29], Li and Kim [30] successfully proposed a reliable and secure ABS scheme under the computational Diffie- Hellman assumption. However, these two schemes only support the restricted forms of signature predicates. The signature length of the above two schemes grows linearly with the size of attributes in the predicate. In addition, Escala*et al*. [31] proposed a revocable ABS for threshold predicate, which shares a similar efficiency with Li *et al.* [30]'s work in signing. Recently, Herranz*et al*. [32] proposed two threshold predicate ABS schemes with a constant size of signature. However, the first scheme requires a large number of extensive computations, and the second one involves $O(d2)$ exponentiations in signing, where d is the upper bound of the threshold value.Considering more expressive predicate, beyond the previous work in [6], Maji*et al*. [33] proposed a general framework for constructing ABS scheme. They showed three instantiations of monotonic predicates which can be dealt under standard secure assumptions. Based on dual pairing vector spaces, Okomato and Takashima [34] proposed the first fully secure ABS scheme to support the general non-monotone predicate. Then, they built an ABS scheme [35] with similar features in the multi-authority settings. Herranz*et al*. [32] observed that the signature size of all previous ABS schemes grows linearly with the number of attributes. So, they presented two threshold ABS schemes with a constant size of the signature. In particular, the second scheme enjoys the unique feature of supporting large universes of attributes. Although the existing ABS requires a large number of modular exponentiations in signing and the complexity usually grows linearly with the size of the predicate formula in threshold ABS, it is very useful in the private access control, anonymous credentials and trust negotiations etc. applications.

2.3 Attribute-Based Signcryption

The first ABSC was proposed by Gagn'eet al. [7] with formal security definitions of messageconfidentialityand ciphertextunforgeabilityfor signcryption in attributebased setting. In order for users to provide different rights for signature and decryption, signing attributes are separated to decryption attributes. Later, Emura*et al*. [36] designed an ABSC scheme with dynamic property that allows updating the signing access structures without reissuing users' secret keys. The signature part makes use of access trees whereas AND-gate policies are used in encryption and decryption process. Wang *et al*. [37] proposed another ABSCscheme by adopting access trees for both signature and encryption parts. The security of [37] is given in the generic group model and random oracle model. By considering the drawbacks of random oracle model, the schemes in [7] [36] are proved to be secure in the standard model. Hu *et al*. [38] suggested a fuzzy ABSC in order to introduce authenticated access control in body area network, whereas no formal security proof for ciphertextunforgeability is provided in existing security models. Ciphertextsize in all of these schemes are increasing linearly with the sum of required signing and encryption attributes. Moreover, the number of expensive bilinear pairing computations are also linear to the number of required attributes. Recently, attributebased ring signcryption [39] and traceable attribute-based signcryption [40] are also proposed respectively. Rao*et al*. [41] proposed an ABSC scheme with the constant size ciphertext using the technique of key-policy ABS. Liu *et al*. [42] proposed a CP-ABSC for PHR system based on CPABE [43] and ABS [33]. However, the CP-ABSC [42] didn't achieve the property of public cipher text verifiability.

III. METHODOLOGY

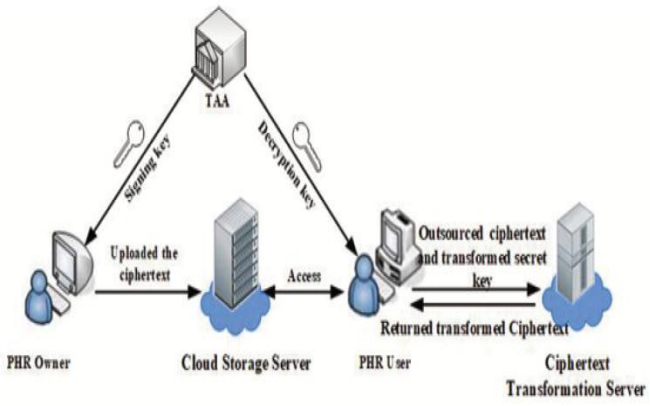

Fig. 2: Architecture of CP-OABSC scheme

This paper consists of 5 modules, which are,

1.Patient/User Creation Module:In this module admin going to create patient/user with valid details and for every patient admin going to create encryption and decryption keys using asymmetric algorithm.

2.Key Generation Module: In this module admin going to generate two keys for encryption and decryption process. By using Asymmetric algorithm RSA, admin going to generate public and private key and stored in the server.

3.User Creation and Mail Sending Module: In this module Data owner going to create users, while creating users private key is created for different users, In the private key attribute-based information of user and private key of data owner is encrypted with the help of DES algorithm and sent to user mail id using SMTP protocol.

4). Upload file to Cloud Storage Module: Data Owner has to select the file from system and click to upload option. So file has to get encrypt by using the RSA public key and after that the encrypted file has to be stored in the cloud storage.
Data owner has to give the file access control for each file. Like this dept, designation peoples can able access this file, this called access policy control.

5). Download file: User has to give private key which is downloaded from mail id, decrypt the private key using DES algorithm and get the information about attributes of user. If user attributes and file attribute is matched means, the file has to be downloaded from cloud storage and after downloaded from cloud, this system has to decrypt the file using RSA Private Key and give it that decrypted file to the user.

IV. PRELIMINARIES

System Model of CP-OABSC.
The architecture of scheme is illustrated in Fig. 2. In our scheme, the PHR owners upload the signcryptedciphertext to the Cloud Storage Server (CSS) which is assumed to be fully trusted. PHR users want to access the PHR data stored on the CSS, they must use their own attribute set to verify whether or not it is satisfy the access policy.The PHR user can verify the correctness of transformation ciphertext, and retrieve the plaintext by its private key and secret value. The proposed CP-OABSC scheme consists of the following algorithms:

1) **Setup** (1λ): The **Setup** algorithm is run by the Trusted Attribute Authority (TAA), which takes security parameter λ, attribute universe A as inputs. Then, it outputs the public parameters PK and a master secret key MSK.

2) **DecKeyGen**(PK,MSK,θd): The TAA takes MSK, PK and an attributes set θdas inputs. Then, it outputs the decryption key SKθdfor PHR user.

3) **DecKey**blind(SKθd): The PHR user takes a decryption key SKθdas inputs. Then, it outputs the transformation secret key TSKθdand the retrieving secret key RSKθd.

4) **SignKeyGen**(PK,MSK,θs): The TAA takesMSK, PK and an attributes set θsas inputs. Then, it outputs the signing key SKθsfor PHR owner.

5) **SignKey**blind(SKθs): The PHR user takes a signing key SKθsas inputs. Then, it outputs the transformation secret key TSKθsand the retrieving secret key RSKθs.

6) **Signcrypt**(PK,Mphr,SKθs,χs,χe): The **Signcrypt**algorithm is run by a PHR owner, which takes thepublic parameters PK, a PHR file Mphr, signer'sattribute set θs, signing key SKθs, signing predicateχsand encryption predicate χeas inputs. Only inthe case of θssatisfies χswhere χs(θs) = 1, the PHRowner can signcrypt the PHR data Mphr. Finally,it will generate a ciphertextSCTχesuch that onlythe PHR user who possesses a set of attributes θdwhich satisfies χewill be able to designcrypt thecorresponding ciphertext.

7) **Designcrypt**user(PK,SCTχe,χs,SKθd): The PHR user takes PK, an attribute set θd, a ciphertext
SCTχeand the decryption key SKθdcorresponding to θdas inputs. Then, it outputs the plaintext Mphror a reject symbol $\perp$.

8) **SignVerify**out(PK,TSKθs,SCT′): The CTS takes PK, a transformation secret key TSKθsand a partial ciphertextSCT′ as inputs. Then, it outputs a
verification result V R for PHR user.

9) **Decrypt**out(PK,TSKθd,E1,E3): The CTS takesPK, a partial ciphertextE1 and E3, a transformation secret key TSKθdas inputs. Then, it outputs a transformed ciphertextTCT for PHR user.

10) **DecSignVerify**user(RSKθd ,RSKθs , TCT, V R): The PHR user takes the retrieving secret keyRSKθdand RSKθs, a verification result V R anda transformed ciphertext*TCT* as inputs. Then, itoutputs a plaintext *Mphr*or a reject symbol $\perp$..

V. CONCLUSION AND FUTURE SCOPE

For eliminate the computational overhead of the designcryption process at PHR user side, we studied the attributed based signcryption scheme [8] and presented an efficient and secure CP-ABSC with verifiable outsourced designcryption scheme. It greatly improves the efficiency of Personal Health Record system and provided the security proof to show that our scheme is CPA-secure. And the experimental evaluation result demonstrates that the proposed scheme is secureand practicable.

ACKNOWLEDGMENT *(HEADING 5)*

We extend our deep sense of sincere gratitude to Dr. K Channakeshavalu, Principal, East West Institute of Technology, Bengaluru, for having permitted to present a project phase-1 on "EFFICIENT SIGNCRYPTION WITH VERIFIABLE DESIGNCRYPTION FOR SHARING PERSONAL HEALTH RECORDS"successfully**.** We express our heartfelt sincere gratitude to Dr.ArunBiradar, Professor and Head, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, for his valuable suggestions and support. We would like to thank our guide Mr.Jagadeesh B N Assistant Professor, CSE Dept, East West Institute of Technology for providing the facilities.

REFERENCES

[1] A. Sahai, B. Waters et al., "Fuzzy identity-based encryption." In Eurocrypt, vol. 3494. Springer, 2005, pp. 457–473.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communicationssecurity. Acm, 2006, pp. 89–98.
[3] A. B. Lewko and B. Waters, "Unbounded hibe and attribute-based encryption." in Eurocrypt, vol. 6632. Springer, 2011, pp. 547–567.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Security and Privacy, 2007.SP'07.IEEE Symposium on. IEEE, 2007, pp. 321–334.
[5] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption." in Eurocrypt, vol. 6110. Springer, 2010, pp. 62–91.
[6] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance."IACR Cryptology ePrint Archive, vol. 2008, p. 328, 2008.
[7] M. Gagn´e, S. Narayan, and R. Safavi-Naini, "Threshold attributebasedsigncryption." in SCN, vol. 6280. Springer, 2010, pp. 154–171.
[8] Y. S. Rao, "A secure and efficient ciphertext-policy attribute-based signcryption for personal health records sharing in cloud computing," Future Generation Computer Systems, vol. 67, pp. 133–151, 2017.
[9] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Transactions onInformation Forensics and Security, vol. 8, no. 8, pp. 1343–1354, 2013.
[10] B. Qin, R. H. Deng, S. Liu, and S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption," IEEE Transactionson Information Forensics and Security, vol. 10, no. 7, pp. 1384–1393, 2015.
[11] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attributebased encryption with verifiable outsourced decryption," IEEETransactions on Information Forensics and Security, vol. 10, no. 10, pp. 2119–2130, 2015.
[12] X. Mao, J. Lai, Q. Mei, K. Chen, and J. Weng, "Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption," IEEE Transactions on Dependable and SecureComputing, vol. 13, no. 5, pp. 533–546, 2016.
[13] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Transactions onParallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.
[14] H. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," IEEE Transactions on Dependable and SecureComputing, 2015.
[15] W.Wu, Y. Mu,W. Susilo, and X. Huang, "Server-aided verification signatures: Definitions and new constructions," in InternationalConference on Provable Security. Springer, 2008, pp. 141–155.
[16] S. S. Chow, M. H. Au, and W. Susilo, "Server-aided signatures verification secure against collusion attack," Information Security
Technical Report, vol. 17, no. 3, pp. 46–57, 2013.
[17] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Annual International Cryptology Conference. Springer, 1991, pp. 129–140.
[18] M. Green, S. Hohenberger, B. Waters et al., "Outsourcing the decryption of abeciphertexts," in USENIX Security Symposium, vol. 2011, no. 3, 2011.
[19] J. Xu, Q. Wen, W. Li, and Z. Jin, "Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing," IEEE Transactions on Parallel and DistributedSystems, vol. 27, no. 1, pp. 119–129, 2016.
[20] R. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," Journal ofSystems and Software, vol. 125, pp. 344–353, 2017.
[21] H. Wang, D. He, J. Shen, Z. Zheng, C. Zhao, and M. Zhao, "Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing," Soft Computing, pp. 1–11, 2016.
[22] J. Li, X. Lin, Y. Zhang, and J. Han, "Ksf-oabe: outsourced attributebased encryption with keyword search function for cloud storage," IEEE Transactions on Services Computing, 2016.
[23] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and finegrained attribute-based data storage in cloud computing," IEEETransactions on Services Computing, 2016.
[24] J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable outsourced decryption of attribute-based encryption with constant ciphertext length," Security and Communication Networks, vol. 2017, 2017.
[25] H. Wang, D. He, and J. Han, "Vod-adac: Anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud," IEEE Transactions on Services Computing, 2017.
[26] A. Burnett, F. Byrne, T. Dowling, and A. Duffy, "A biometric identity based signature scheme."IJ Network Security, vol. 5, no. 3, pp. 317–326, 2007.
[27] P. Yang, Z. Cao, and X. Dong, "Fuzzy identity based signature."IACR Cryptology EPrint Archive, vol. 2008, p. 2, 2008.
[28] G. Shanqing and Z. Yingpei, "Attribute-based signature scheme," in Information Security and Assurance, 2008.ISA 2008.InternationalConference on. IEEE, 2008, pp. 509–511.

Authors Profile

Mr. CHETHAN V pursuing Bachelor of Computer Science And Engineering from VisvesvarayaTechnologicalUniversity

Mr.VIJAY KUMAR N pursuing Bachelor of Computer Science And Engineering from VisvesvarayaTechnologicalUniversity

Mr.KARANDEEP S.V pursuing Bachelor of Computer Science And Engineering from VisvesvarayaTechnologicalUniversity

Ms.PALLAVI N pursuing Bachelor of Computer Science And Engineering from VisvesvarayaTechnologicalUniversity

Mr.JAGADEESH BN pursued Mtech in Computer Science And Engineering from VisvesvarayaTechnologicalUniversity

