AN EFFICIENT KEYWORD SEARCH AND DATA SHARING SCHEMES IN CLOUD COMPUTING

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

AATIKA FATIMA (19S41D5801)

Under the Guidance of
Dr.D.SRINIVAS REDDY
Assoc. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "AN EFFICIENT KEYWORD SEARCH AND DATA SHARING SCHEMES IN CLOUD COMPUTING" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

AATIKA FATIMA (19S41D5801)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

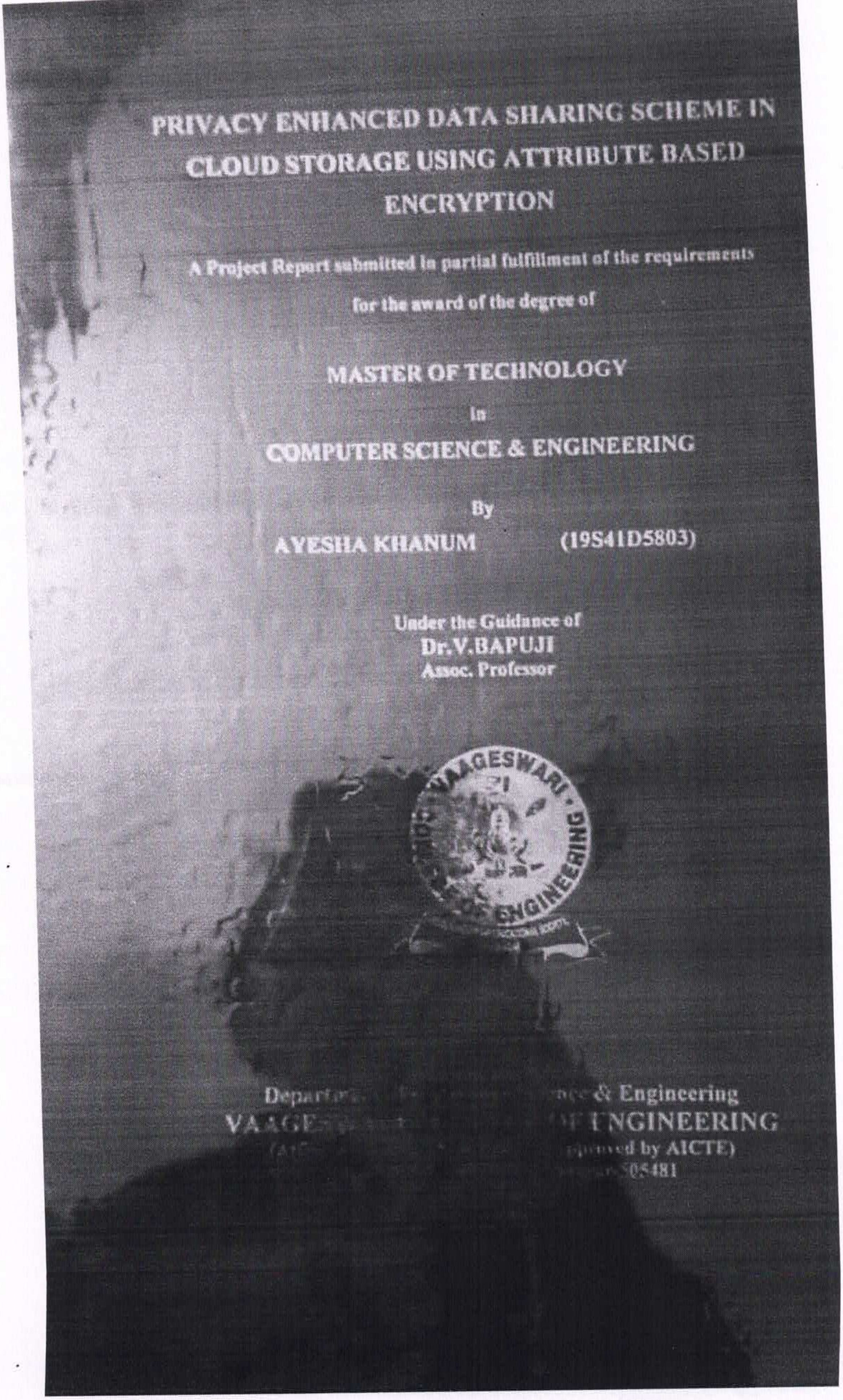
Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

Cloud infrastructure adoption has significantly reduced hardware and software infrastructure cost. Normally data are encrypted to preserve security before they are transported into the cloud. After encryption, data is more difficult to locate and exchange than raw data to find and transmit. On the other hand, the cloud provider plays an essential role as clients want the cloud to find results and swiftly return findings. We propose a guideline for the search and exchange of encrypted cloud data (CPAB-KSDS). The solution offers search of keywords on the basis of characteristics and attribute-based data exchange. In sharing without the PKG the keyword in our system can also be updated. The concept and safety model of CPAB-KSDS are discussed in this document. We also have a random oracle system and prove that an attack on a ciphertext and a picked keyword is safe. The proposed construction is practical and efficient in terms of performance and property comparison.

CHAPTER-8
CONCLUSION

A novel concept, the Cyprus text policy mechanism, is introduced in this study, which can be used for the search and exchange of data (CPAB-KSDS). A random oracle and a concrete CPAB-KSDS system are being used in this study to demonstrate the safety of the systems. The proposed approach is efficient and practical in terms of performance and property comparisons. When it comes to attribute-based keyword searches and encryption, this article provides a good solution that does not require the use of PKG during the joint phase. Our research also leads to some intriguing challenges, such as the development of a CPAB-KSDS scheme that does not rely on random oracles or the development of a new system for more expressive searches.



PRIVACY ENHANCED DATA SHARING SCHEME IN CLOUD STORAGE USING ATTRIBUTE BASED ENCRYPTION

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

AYESHA KHANUM (19S41D5803)

Under the Guidance of
Dr.V.BAPUJI
Assoc. Professor

Departm[illegible] [illegible]nce & Engineering
VAAGE[illegible] [illegible] ENGINEERING
(A[illegible] [illegible]pproved by AICTE)
[illegible]505481

Principal
Vaageswari College of Engineering
[illegible]NAGAR-505 527.

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "PRIVACY ENHANCED DATA SHARING SCHEME IN CLOUD STORAGE USING ATTRIBUTE BASED ENCRYPTION" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

AYESHA KHANUM (19S41D5803)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

ABSTRACT

Data sharing is a practical and inexpensive solution to the cloud. The privacy of data is further undermined when it is outsourced to a number of cloud servers. Various techniques to tighten data access control in order to secure essential and sensitive information are being tested. It can be easier to preserve and encrypt text policy characteristics with text (CP-ABE) (CP-ABE). The CP-ABE standard focuses mainly on data confidentiality; however user privacy is a significant problem at present. The CP-shrouded ABE Access Policy also guarantees data confidentiality and user privacy. On the other hand, most modern methods are inefficient in terms of total communication and expenditure calculation. Moreover, during the authority check, most projects do not contain the power verification or the concern about the privacy leakage. This work provides a powerful CP-ABE system based on competencies which respects personal confidentiality to address the abovementioned difficulties. There are also a number of secret keys. While this technique provides sélective certainty and the decisional linear assumption to the key n-BDHE issue. The calculation findings support the worth of the proposed system.

CHAPTER-8
CONCLUSION

We introduced a CP-ABE technique as an alternative to the usual model that preserves privacy. Many enhancements over prior systems are provided by the technology described here, including constant-size private keys and a short text cypher. It only takes four pairing calculations to complete the decryption process. The proposed technique in a high order group ensures a certain level of safety and anonymity for the participants. We demonstrate in the standard model that the safety of the system proposed can be reduced to the two critical assumptions, n-BDHE and DL, by simplifying the system. Additionally, the approach offers to check the authorisation and avoid the leakage of personal information.

Although only "AND" policies were supported by the system, the system was built on a defective safety concept. It is anticipated that future study would examine how a robust and secure HP CP-ABE may be built with more flexible access controls.

DYNAMIC AND SECURE CLOUD STORAGE USING NETWORK CODING TECHNIQUES

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

SUSHMITHA EJJAGIRI (19S41D5805)

Under the Guidance of
Dr. N.CHANDRAMOULI
Assoc. Professor & HOD

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad & Approved by AICTE)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"DYNAMIC AND SECURE CLOUD STORAGE USING NETWORK CODING TECHNIQUES"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

SUSHMITHA EJJAGIRI (19S41D5805)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

Storage space is restricted. In the age of cloud computing, users have the ability to externalise data to remote servers. Instead of monetary compensation, these servers may always retrieve data from their customers. Secure cloud storage systems allow users to keep track of the integrity of their data while it is being stored elsewhere. In this study, we look at how secure and dynamic data cloud storage may be developed using secure network encoding approaches. It is demonstrated that a large number of safe network coding schemes can be employed to construct quick and dynamic data cloud storage protocols, and it is also created that a secure network coding protocol is used (DSCS I). Incorporating safe network coding techniques into the standard paradigm, DSCS I is the first secure cloud storage protocol for dynamic data to be designed. To the best of our knowledge While dynamic data in general allows for endless additions, deletions, and changes, add-only data can be produced in a variety of real-world applications. DSCS II cloud storage protocol for add-only information is being developed to solve some of the limitations of DSCS I. Finally, we provide prototype implementations of DSCS I and DSCS II in order to evaluate their performance.

CHAPTER-8

CONCLUSION

In this study, we suggested a secure DSCS that is based on the SNC secure protocol (Dynamic Data Cloud Storage Protocol). As far as we know, this is the only DSCS protocol based on SNC that has been made secure and verifiable publicly in the Standard Protocol. We discussed some of the difficulties in developing a good DSCS protocol for the SNC protocol. As a result, we discovered a number of flaws in a dynamic cloud storage system built on SNC. Nonetheless, some of these restrictions apply to the core SNC protocol that was employed. A more efficient DSCS protocol could be achieved by the improvement of the SNC protocol. Aside from that, we've developed a number of SNC-only data techniques as well as an efficient DSCS (DSCS II) data-only protocol. We have demonstrated that DSCS II overcomes a number of DSCS I limitations. The prototype implementations of DSCS I and DSCS II were created for the purpose of demonstrating their feasibility and comparing the performance of DSCS I with the performance of an SNC-based secure cloud storage system for static data and the performance of DPDP II.

AN EFFICIENT SECURE DATA STORAGE IN CLOUD USING REVOCABLE ATTRIBUTE BASED ENCRYPTION

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

FARAZ FATHIMA (19S41D5806)

Under the Guidance of
MD.SIRAJUDDIN
Assoc. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "AN EFFICIENT SECURE DATA STORAGE IN CLOUD USING REVOCABLE ATTRIBUTE BASED ENCRYPTION" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

FARAZ FATHIMA (19S41D5806)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER PRINCIPAL

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

The number of people who use mobile devices to access cloud-specific data is increasing. For privacy and data protection, cloud storage solutions typically employ attribute-based encryption (ABE). One of the most significant efficiency limitations of ABE is the high overhead processing and data access on mobile devices during user revocation. In order to address these issues, we propose a revocable RADS solution with some intriguing features. Our RADS solution enables beginners to improve access control systems so that file owners are unable to expressly define their external files with permissible visitors. Second, our RADS technology enables mobile users to share time-consuming file access computations with the cloud service provider without disclosing the contents of the files in the process (CSP). Our RADS System, in addition to offloading access credentials and CSP re-encryption activities throughout the revocation process, ensures that no users are left without a revocation. RADS Revocation improves security by preventing revoked users from accessing files that are older or newer than they are allowed to access. The results of the testing and analysis of the RADS system's safety and effectiveness have been confirmed.

CHAPTER-8
CONCLUSION

We design a primary CPABE system in this project. The validity is determined by the occurrence in generic group patterns of random oracles[29]. The efficiency of the programmes and speed at which group actions may be carried out justify primary groupings. The composite group system based on enhanced safety principles of the dual system encryption model can be nonetheless useless when it comes to creating our structure[42]. We're going to pause it for the moment. The following queries (with or without revocation) can be answered by this document: Part IV describes multi-authority decryption for online CPABE decryption and part V talks about offline CPABE decryption (Appendix VIII) and offline outsourcing of multiauthorities (Appendix VIII). The disadvantage of outsourcing decryption is that a user cannot partially decode. As a remedy to this problem, verifiable outsourcing[25] was offered. Under our circumstances, confirmed outsourcing can be addressed using a similar technique. We are not going to talk about it because we stick to an honest yet curious strategy. When this assumption has proven erroneous, certified outsourcing of decryption should be considered. We will leave that open. We will leave that open. The paper describes a versatile and reliable ABE mobile cloud architecture. Decentralization benefits, fast encryption, external decryption and user notifications can be combined. Due to the fact that all encryption is done offline, decentralised ABE systems are faster and more efficient than central ABE. A rogue proxy server partially decrypts encryption, but the outcome is no information. Data customers can decrypt cypher code text fully without the use of pricey combination techniques. Our solution allows users to cancel without any huge additional charges during the online transaction. Our solutions offer the best encryption and decryption performance compared to other systems, together with the most useful features, like decentralisation and user revocation.

ENHANCED SECURITY SCHEMES IN CLOUD USING BIOMETRIC BASED ACCESS

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

KULSUM SUBIYA (19S41D5808)

Under the Guidance of
MD.SIRAJUDDIN
Assoc. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to [illegible] & approved by AICTE)
Ram[illegible] Karimnagar-505481
[illegible]

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "**ENHANCED SECURITY SCHEMES IN CLOUD USING BIOMETRIC BASED ACCESS**" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

KULSUM SUBIYA **(19S41D5808)**

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

ABSTRACT

Remote storage and computer services are in high demand in today's data-driven culture, as they allow for secure access to data and services. This article describes a biometric authentication approach for securing remote (cloud) server access, as well as some of the challenges involved. The biometric data of a user is considered confidential in the methodology that has been proposed. Biometric data is used to create an individual's unique identity and private key, which are both stored on a secure server. Also included is an explanation of how to create a secure message session key between two communication partners using two different biometric templates. In other words, if at all possible, neither the private key nor the session key should be retained until further information is provided. In order to ensure formal safety, the methodology relies on rigorous formal and random analyses, as well as non-mathematical checks. This can be generated automatically using an ISP/AC tool (AVISPA). Finally, numerous tests and comparative studies are carried out in order to demonstrate the effectiveness and utility of the concept.

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

CHAPTER-8

CONCLUSION

The use of biometric security systems is becoming increasingly popular, and they offer significant advantages over traditional password and token systems (such as those found on iOS and Android devices) (e.g., on Android and iOS devices). Throughout this paper, we have discussed a mechanism for the biometric authentication of users who have remote access to a computer and its associated services. Given that a fingerprint can be used to generate 95.12 percent of the same key, our proposed method allows for the generation of private keys from biometric fingerprint information. For our proposed session method, which makes use of two biometric data points, there is no need for any prior information exchange. When compared to a number of similar authentication protocols to a number of well-known attaches, we find ours to be more resilient.

Future improvements

The use of additional biometrics, particularly multi-modal biometrics, should be investigated in more sensitive applications (for example, domestic security issues) (e.g., in national security matters).

ENHANCING THE CLOUD SERVICES AND PRIVACY WITH SEARCHABLE ENCRYPTION SEARCH PATTERN

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

SOUMYA METHUKU (19S41D5809)

Under the Guidance of
Dr. N.CHANDRAMOULI
Assoc. Professor & HOD

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad & Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad & Approved by AICTE)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "ENHANCING THE CLOUD SERVICES AND PRIVACY WITH SEARCHABLE ENCRYPTION SEARCH PATTERN" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

SOUMYA METHUKU (19S41D5809)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

It is the primary goal of this research to use a single term to search for sensitive material in a cloud environment. In some cases, the reliability of cloud service providers cannot be guaranteed. Consequently, the information must be provided to a third party in an encrypted format. Create and deliver cloud tokens in order to search for a term by authorised users (ABKS). It is possible to obtain cipher texts at any time by using the search tools available. Giving a technique in which search tokens can remove only cipher texts that have been formed within a specific timeframe as a result of information leakage would be optimal. The KPABTKS basic encryption keyboard, which we developed to accomplish this, was introduced. There is nothing particularly fast about the keyword search. Our proposed solution is formalised in terms of its safety against the selective attack using a random oracular model and the rigour of the Diffie-Hellman decision-making process (DBDH) (SCKA). It is also dependent on the number of attributes used in the encryption process whether there is an issue. The effectiveness of our plan is demonstrated by your performance rating.

CHAPTER-8

CONCLUSION

The primary component of cloud computing is cloud storage. As a temporary remedy, a search for terms based on critical policy attributes (KPABTKS) has been developed (KPABTKS). Using this technique, any data user can generate a search token that is only valid for a limited amount of time. We made a first specific idea for the new primitive encryption system, which was based on the bilinear map. By utilising the random oracle notion, we have discovered that our system is secure. Because of the large number of features associated with our concept, we use a linearly complex encryption procedure. Furthermore, the number of pairings required by the search algorithms is proportional to the number of search token attributes. The success of our strategy is demonstrated by the practical features of estimating costs and the length of time it will last.

EFFECTIVE STORAGE PROTECTION FOR CLOUD TO PREVENT UNAUTHORIZED ACCESS USING IOT

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

ZEBA SHABNOOR (19S41D5810)

Under the Guidance of
Mr.S.SATEESH REDDY
Asst. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"EFFECTIVE STORAGE PROTECTION FOR CLOUD TO PREVENT UNAUTHORIZED ACCESS USING IOT"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

ZEBA SHABNOOR (19S41D5810)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

As the number of Internet of Things devices grows, new access control solutions will be required to prevent unauthorised access to this type of information. In order to ensure secure information distribution to authorised subscribers, a dynamic Internet of Things environment with rigorous signal monitoring is required. The Key Management Group is the primary mechanism for controlling the dissemination of access keys and the security of protected data (GKM). However, the majority of IoT and GKM access control solutions today are based on centralised technologies that are unable to address skiing issues that arise as a result of the growing number of IoT devices and their users. A further problem is that none of the current GKM systems ensures that members of the same group are independent of one another. They only connect to subsets that have symmetrical group keys, which has proven ineffective for users who are particularly dynamic in their needs. In order to overcome these difficulties, we have developed a specific, lightweight decentralised group architecture that is decentralised in nature (DLGKM-AC). This technique, which is based on the hierarchy of the central distribution centre and the various distribution centres, improves the administrative functioning of the subscribers while also speeding up the KDC rekeying process for them (SKDCs). It has also been developed a new master token management system that can handle a large number of subscribers and will be used for the main distribution. The overheads associated with storage, calculation, and transfer are eliminated by using this protocol. This technique is appropriate for an IoT architecture that can be scaled and reduces the number of fault sites as well as the amount of data transmitted over the central network. DLGKM-AC relies on confidentiality and collusion to maintain communication within a secure group environment. Significant resource gains in overhead storage, measurement, and transmission are demonstrated by the results of the simulation and analyses of the proposed methodologies.

CHAPTER-8
CONCLUSION

This study presents the group-key control mechanism in the dynamic IoT environment which is decentralised within the DLGKM-AC. A single KDC manages and updates group keys while a number of SKDCs directly manage links between the device and its users, leading to a heretic design. A new master token encryption system has also been developed to protect the independence of participants in highly dynamic group discussions. With retroactive and future confidentiality and minimal rehabilitation, mobility within the DLGKM-AC is simply regulated. Our solution also tackles the 1-effects-n problem. Even if an SKDC is involved, customers always have access to data. There is also a detailed safety analysis of a wide range of desired safety elements. Furthermore, the performance test shows that our recommended solution performs better than others by reducing overhead storage, transmission and processing costs. Finally, decentralised architecture enhances the scalability and overhead reduction of limited resources devices. We are already building a Physical Network for users with a range of IoT devices and smart phones in the context of the EU-wide project PARFAIT[28] to implement our architecture in a concept-proof way.

PREDICTION OF COMBINED CYCLE POWER PLANT OUTPUT USING MACHINE LEARNING

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

P.DEEKSHITH CHARY (19S41D5814)

Under the Guidance of

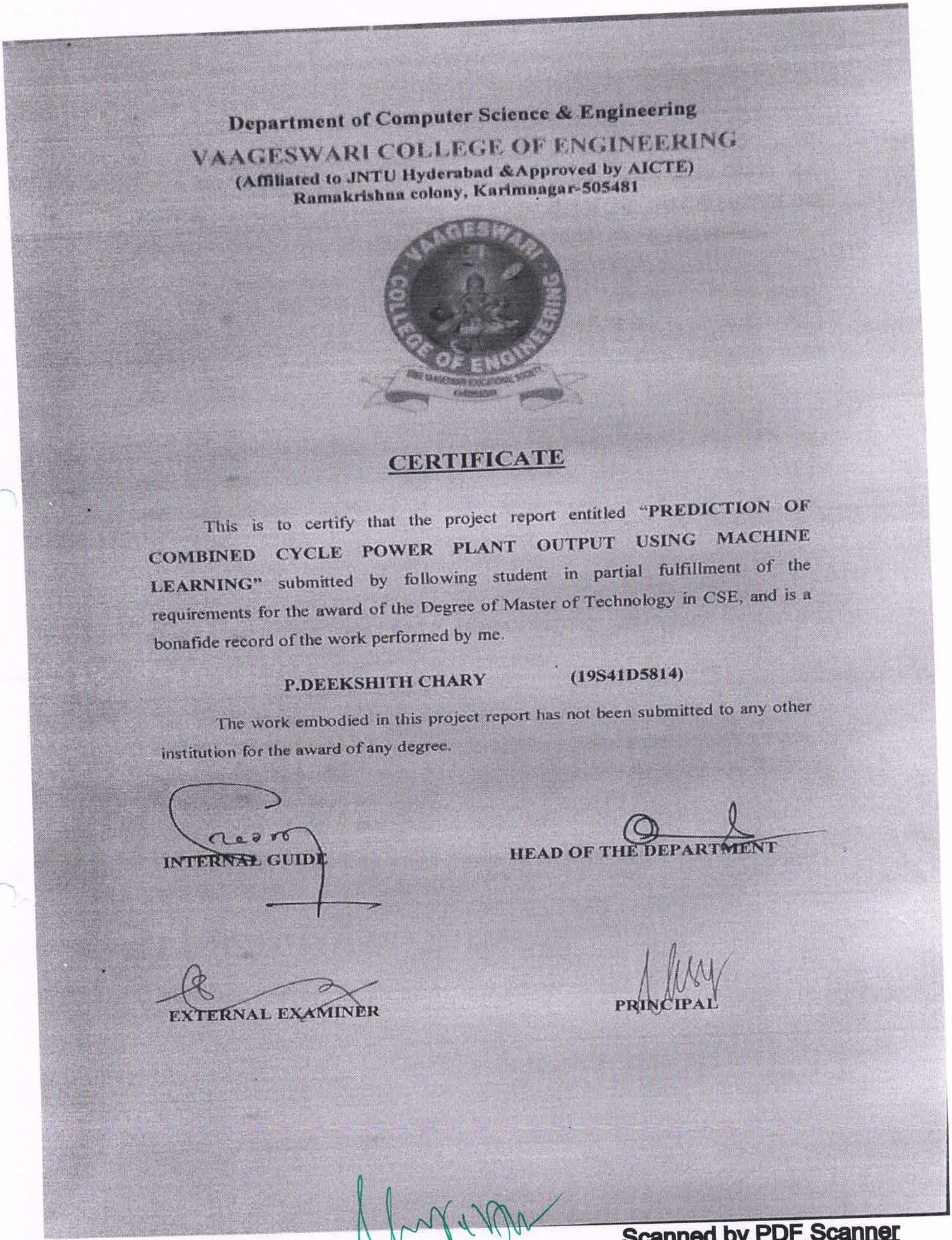
Mr. K.SRIDHAR REDDY

Assoc. Professor

Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022



Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "PREDICTION OF COMBINED CYCLE POWER PLANT OUTPUT USING MACHINE LEARNING" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

P.DEEKSHITH CHARY **(19S41D5814)**

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE HEAD OF THE DEPARTMENT

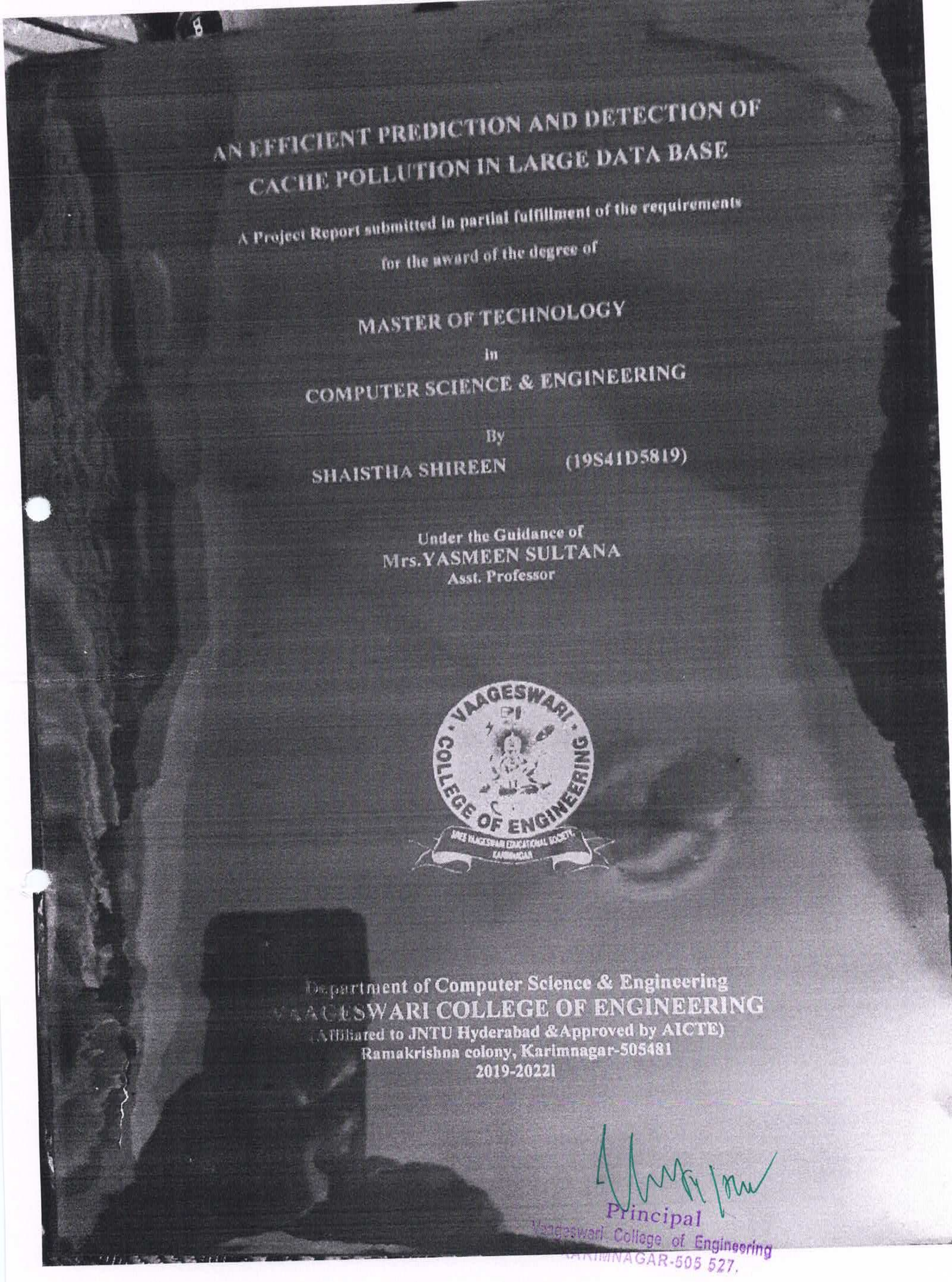
EXTERNAL EXAMINER PRINCIPAL

ABSTRACT

Predicting electrical power made in combined cycle power plants is test in the field of electrical power and energy systems. The base load activity of a power plant is influenced by four fundamental boundaries, which are used as information factors in the dataset, as ambient temperature, atmospheric pressure, relative humidity, and exhaust steam pressure. Thus, the business issue is the best approach to foresee the power creation as a component of these normal conditions, to arrange the advantage. These boundaries affect electrical power output, which is viewed as the goal variable. The dataset has two or three incredible exemptions identified with its four free factors, and these are the expectation precision of AI procedures. Algorithms are for the most part utilized in the prescient assessment of the power plants' evaluated energy creation. The dataset in like manner uncovers basic differentiations in expectation precision achieved for different spaces of the P.E. dispersal. This arrangement perceives that expectation precision could be improved by parcelling the dataset into autonomously progressed subsets, three with its primary P.E. design and a fourth, minuscule subset containing the peculiarities.

12. CONCLUSION

A power plant's productivity has ordinarily insinuated as the power conveyed per energy input. An ideal power orchestrating is crucial for staying aware of the sufficiency between power age and power use. Power plants and Machine learning (ML) are two unmistakable fields. In any case, applying ML algorithms to the data set created by a solidified cycle power plant (CCPP) can join these two fields and bring useful results. In extension to showing its profoundly precise prediction capacities, the CCGT. Thusly, the administrators can expect the exhaust steam vacuum of the S.T., which is fundamental in the S.T. output, with incredible precision. Then, the data was used to expect the power output of the S.T. using data open to the administrators through the power plant's appropriation community. The prediction can be utilized in two ways. In the first place, it very well might be joined in a hearty condition observing system in which the online execution is diverged from the deduced model, and any deviations are dissected and researched. This can ensure secured and trustworthy movement in various conditions. Second, the model can be used for precise power creation gauges. These evaluations are used in the electrical power market. The data set has gigantic exemptions in its variable scatterings. The more huge part is oddities in the prediction bungle apportionment because of their peculiar autonomous variable values.ML algorithms are expected to make a prediction. This judicious brand name can be used in various districts to further develop possibilities in such fields.



AN EFFICIENT PREDICTION AND DETECTION OF CACHE POLLUTION IN LARGE DATA BASE

A Project Report submitted in partial fulfillment of the requirements for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

By

SHAISTHA SHIREEN (19S41D5819)

Under the Guidance of
Mrs.YASMEEN SULTANA
Asst. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022l

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"AN EFFICIENT PREDICTION AND DETECTION OF CACHE POLLUTION IN LARGE DATA BASE"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

SHAISTHA SHIREEN (19S41D5819)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

INTERNAL GUIDE **HEAD OF THE DEPARTMENT**

EXTERNAL EXAMINER **PRINCIPAL**

ABSTRACT

It is impossible to overestimate the importance of variety in the network of opinion polls when it comes to communicating social concerns to the general public. Models for user involvement in various hot social communication settings that take into consideration the interplay between numerous messages and detailed behaviour are available, and these models are the subject of this paper. While attempting to prevent user engagement, this technique also takes into account the potential impact of a high number of communication channels on the overall system. An interactive system that includes a neural backbone system as well as a neural network can be used to foresee societal concerns, user behaviour, and network connectivity, among other things (BP). Furthermore, because the neural BP network's multimodal interactions are iterative, integration is a piece of cake with this network due of its simplicity. The application of a simulated ringing method improves the predictability of the resulting data set. User engagement in modern interdisciplinary evaluation exchanges was investigated using the model, which looked at the relationships between different messages in order to acquire a better understanding of user participation.

CHAPTER-8

CONCLUSION

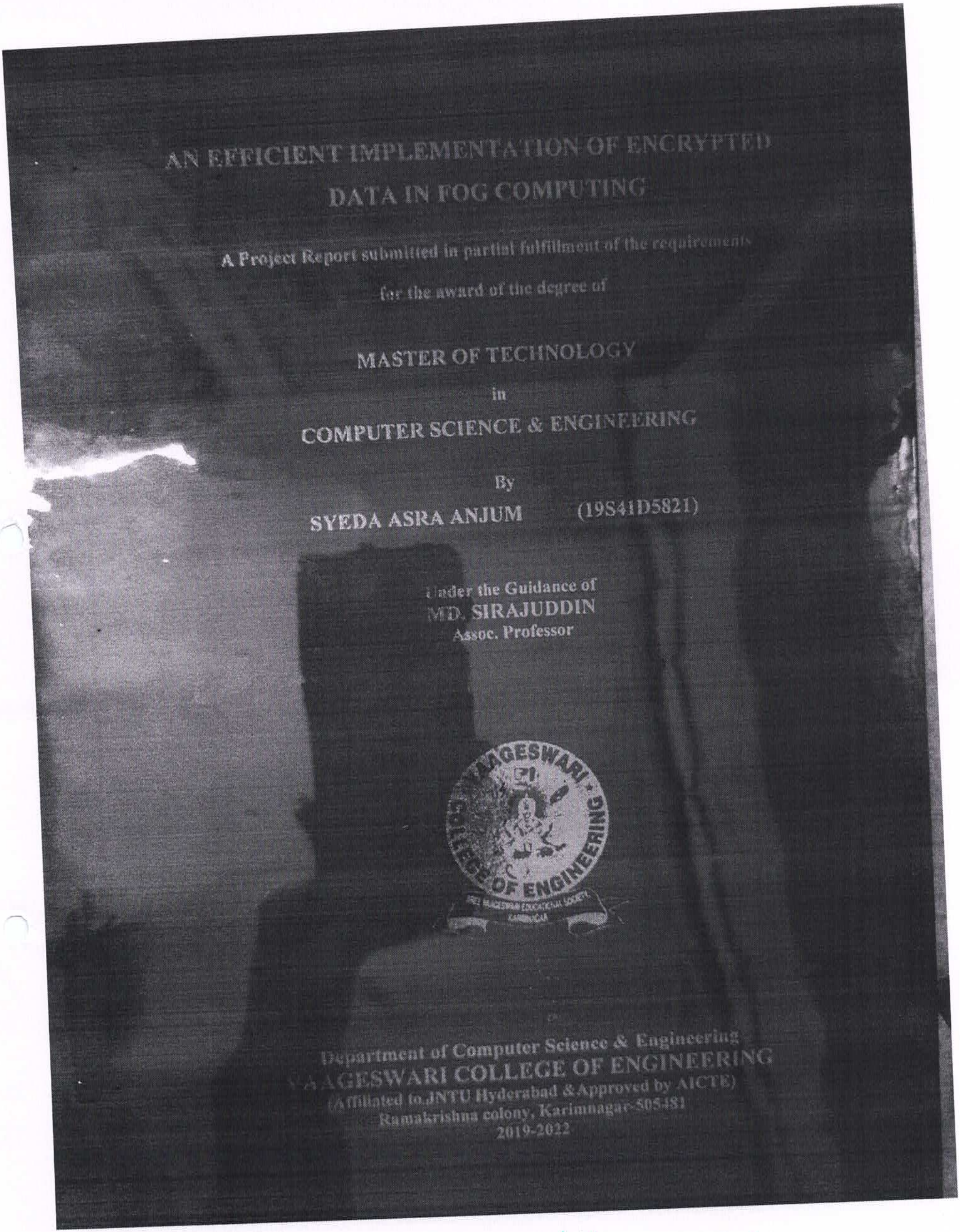
Following the findings of the research, researchers discovered that they could develop a prediction model for engagement on a social networking site based on the behaviour and crucial information provided by users of the site, using data from a popular problem addressed on the site, according to the findings.

In order to account for the various nonlinear linkages between users' driving processes and the multi-message interaction, a Bayesian neural network model (BP neural network) was developed to forecast user participation behaviour. Iterative training on user behaviour was triggered as a result of the problem, and the BP neural network suffered as a result of overfitting as a result of the training.

A simulated annealing technique was used to address overfitting, which resulted in a considerable improvement in the accuracy of the forecast. Through the use of multiple-message correlation measurements and statistical analysis of model outputs, we were able to calculate the percentage of users that participated in one message and also participated in other messages.

It was discovered that the computation findings accurately reflected the repercussions of a hot subject on user engagement behaviour since they were predicated on estimates of the mutual effect strength between the numerous messages provided to participants, which were then validated by the researchers.

When the proposed approach was tested on a big batch of multi-message data from a popular Sina Weibo subject with a large number of messages, it was discovered that it performed well and was cost-effective. Our ability to accurately predict user behaviour as well as the level of mutual influence between numerous communications that happened over a short period of time was made possible by the model's accuracy. Ultimately, it was as a result of this evolution that media outlets did not ignore the quick shifts in public opinion on what was previously an extremely polarising issue.



AN EFFICIENT IMPLEMENTATION OF ENCRYPTED DATA IN FOG COMPUTING

A Project Report submitted in partial fulfillment of the requirements for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

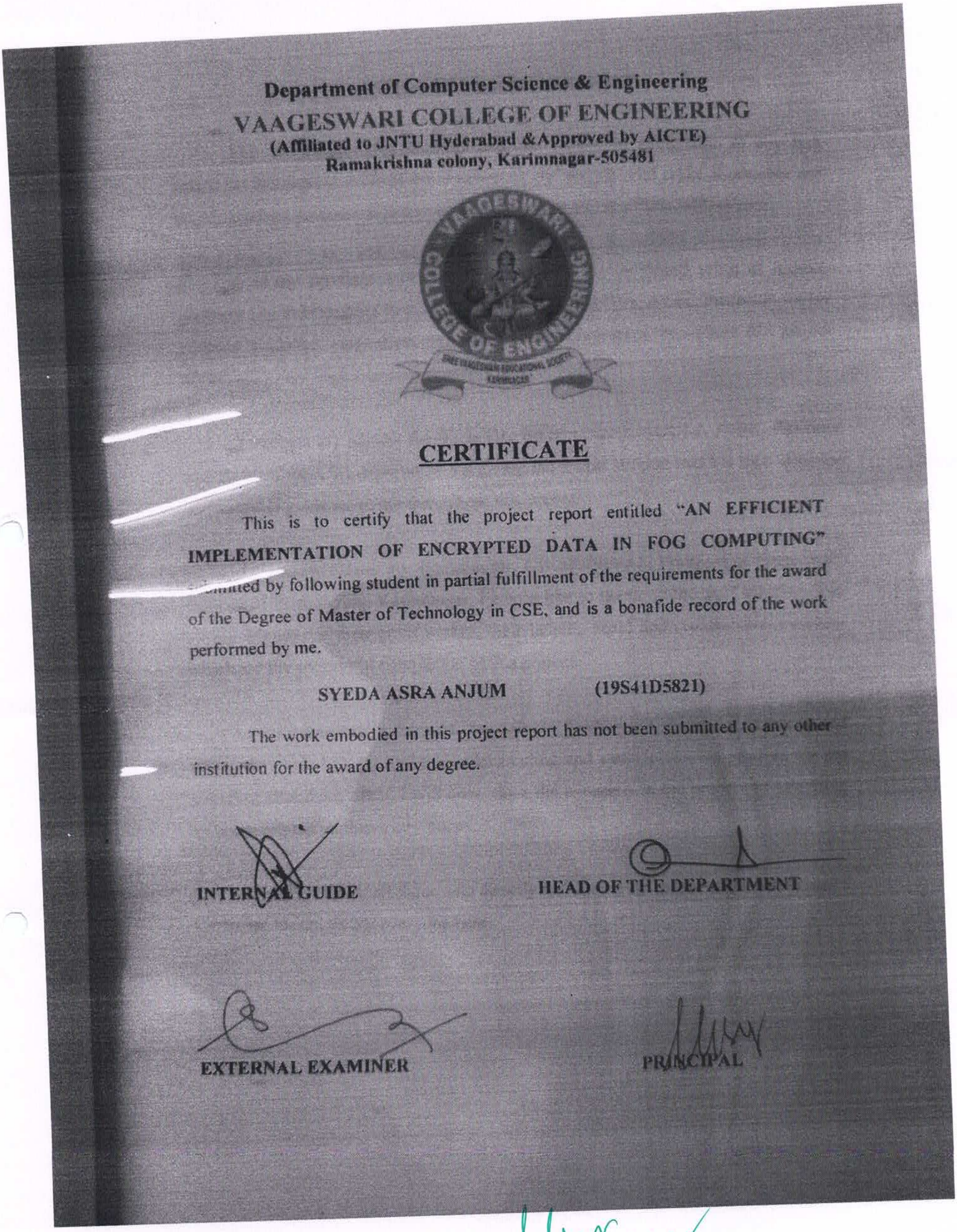
By

SYEDA ASRA ANJUM (19S41D5821)

Under the Guidance of
MD. SIRAJUDDIN
Assoc. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to JNTU Hyderabad & Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.



Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad &Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled "AN EFFICIENT IMPLEMENTATION OF ENCRYPTED DATA IN FOG COMPUTING" submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

SYEDA ASRA ANJUM (19S41D5821)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

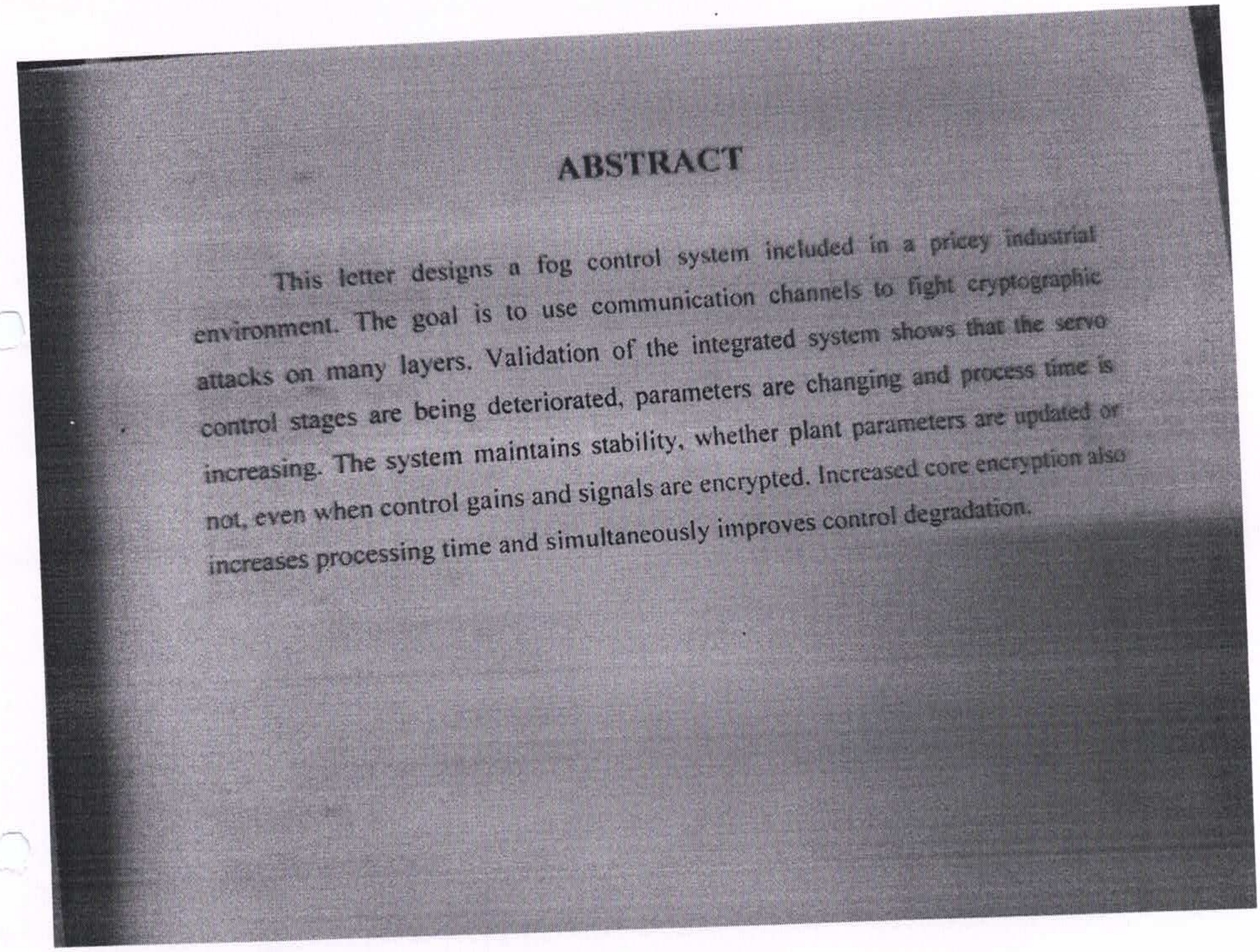
INTERNAL GUIDE HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER PRINCIPAL

Principal

Vaageswari College of Engineering

KARIMNAGAR-505 527.



ABSTRACT

This letter designs a fog control system included in a pricey industrial environment. The goal is to use communication channels to fight cryptographic attacks on many layers. Validation of the integrated system shows that the servo control stages are being deteriorated, parameters are changing and process time is increasing. The system maintains stability, whether plant parameters are updated or not, even when control gains and signals are encrypted. Increased core encryption also increases processing time and simultaneously improves control degradation.

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

CHAPTER-8

CONCLUSION

This letter discusses an encoded control system based on a secure fog-based system originally employed as an encoded controlling system for the industrial environment. The intended audience for this book are engineers and scientists. The opponents do not grasp the control and retention signals. The approach is intended to protect against attacks and zero dynamic circumstances. As can be seen in this example, in addition to the existing security measures, the control encryption approach for industrial control systems can be employed as an additional protective layer.

As the test results show, the significant processing time has to do with the efficiency of the monitoring of load fluctuations. Controller encryption as specified in Sections IV-A and IV-B is provided. Given the deteriorating safety and control performance, the key length should be as long as possible. However, the findings in Section IV-C indicate that in these circumstances the time needed for encryption and decryption is negligible. Hardware encryption and decryption solutions are therefore needed for facilitating the use for resource limited applications of encrypted control systems (for example, by using a programmable array of field doors).

As a result of a future study of high layer control, a fog-based cloud control system will be developed in the coming years. A Denial of Service (DDOS) attack and counterfeiting and other malicious forms have been conducted[19].

PRIVACY ENABLED MEDICAL DIAGNOSIS IN ENDGE COMPUTING

A Project Report submitted in partial fulfillment of the requirements

for the award of the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

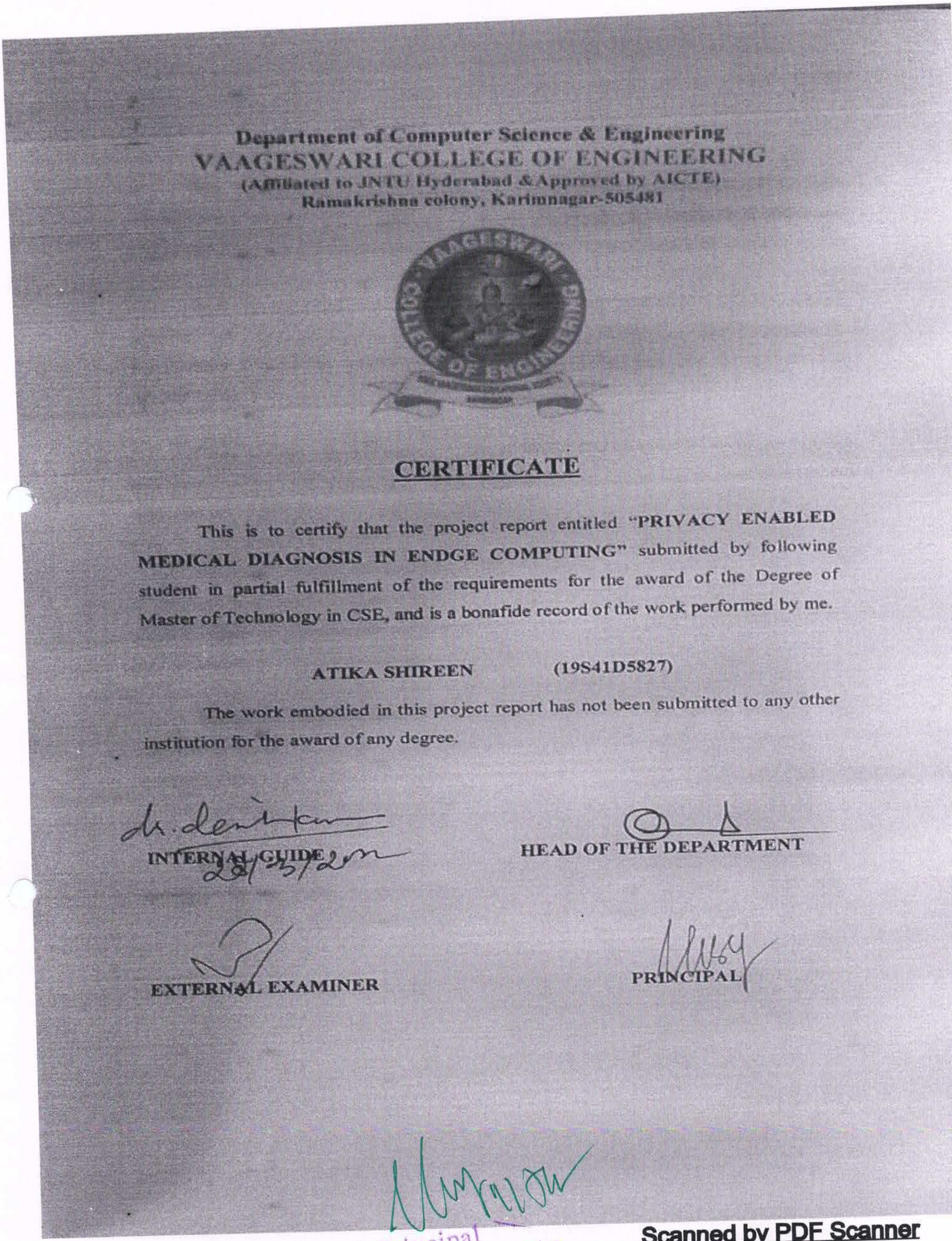
By

ATIKA SHIREEN (19S41D5827)

Under the Guidance of
Dr. DINESH KUMAR
Assoc. Professor

Department of Computer Science & Engineering
VAAGESWARI COLLEGE OF ENGINEERING
(Affiliated to ~~JNTU~~ Hyderabad &Approved by AICTE)
Ramakrishna colony, Karimnagar-505481
2019-2022

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.



Department of Computer Science & Engineering

VAAGESWARI COLLEGE OF ENGINEERING

(Affiliated to JNTU Hyderabad & Approved by AICTE)

Ramakrishna colony, Karimnagar-505481

CERTIFICATE

This is to certify that the project report entitled **"PRIVACY ENABLED MEDICAL DIAGNOSIS IN ENDGE COMPUTING"** submitted by following student in partial fulfillment of the requirements for the award of the Degree of Master of Technology in CSE, and is a bonafide record of the work performed by me.

ATIKA SHIREEN (19S41D5827)

The work embodied in this project report has not been submitted to any other institution for the award of any degree.

28/3/2021

INTERNAL GUIDE

HEAD OF THE DEPARTMENT

EXTERNAL EXAMINER

PRINCIPAL

Principal
Vaageswari College of Engineering
KARIMNAGAR-505 527.

ABSTRACT

The growing use of smart phones, cloud computing and cloud technologies has generated huge demand for healthcare. The data collection, storage and dissemination processor cycles are typically utilized, with the exception: data management is done by data acquisition, storage and transmission. Security and expensive energy expenses are some of the concerns of cloud-based medical data administrators. This is a key start to choose the proper data sharing technology. Principally, the health system must be revamped. Because of its privacy, data transfer and intrusion detection systems are both crucial. The first wearable encryption technology in the world (NTRU) (NTRU). Our purpose is to cut energy bills through the exchange of knowledge on the Internet. Until recently, cloud information was only usable in very limited contexts and was scrutinised extremely rigorously by the service provider. Patients trust their doctors to discuss their medical problems with them. We use a range of modes of treatment including cloud computing, electronic records and clinical teams. Our purpose was to develop a network for the detection of these threats. Our approach to the issues is confirmed by our previous experience and our ongoing testing and research.

CHAPTER-8

CONCLUSION

In addition to privacy, XG Boost can download as little data as possible from the internet. Patient information is vital and safe LPME computers cannot work successfully in medical contexts without the necessary patient information. The safety and effectiveness of LPME therapy in real-life clinic situations, commonly called lateral nervous stimulation. The research was published in the journal Neuroscience. In order to determine therapeutic effectiveness and safety, researchers examined real-world clinical data for patients. The results were published following attendance in the Neurology Journal (LPNS).