



Seed money for Research

Need:

Research needs investment of time and money to take a shape in a higher educational institution. In the context of extreme competition for funding from government and private agencies, it is essential for the institution to support and develop their members of faculty to equip themselves with constructive foundation and support for applying for funding as well as publishing in reputed journals. Hence, seed money helps the members of faculty to do some bench work and create basis for a solid and extended proposal to the external funding agency.

Objectives:

- To provide financial support to the members of faculty for undertaking minor research work.
- To support faculty with a small and reasonable grant with which they can jump start their research work.
- To encourage members of faculty to conduct sufficient research work for obtaining 'proof of concept' or 'proof of experience', which further enables them to apply to external public and private funding agencies.

Eligibility:

- All full-time members of faculty of the institution are eligible for this grant.
- The proposed area of research must be novel and very little work have been done.

Process:

- Interested faculty must submit their proposal in the detailed format to the principal.
- The principal refers the proposals to the Research Advisory Committee for scrutiny and review of the proposal.
- Faculty of the institution can collaborate and submit a proposal with one of the principal investigator and other members as co-investigators.

- Only one proposal can be submitted by a faculty per year
- The principal investigators of the shortlisted proposals will be called for a presentation
- The report of the Research Advisory Committee will be released with the final selected proposals
- The rejected proposals can be reworked for resubmission based on the comments/suggestions of the Research Advisory Committee
- All approved proposals will be given a letter of sanction indicating the amount sanctioned and permitted duration of the work
- Quarterly review of the work shall be conducted to monitor the progress made
- After completion of the proposed work, a completion report along with utilization of sanctioned grant should be submitted.
- If possible and sufficient, the results of work should be sent for a publication or apply for a patent.
- Also, the work should be developed further into a full and standard proposal for applying to a public or private funding agency.

Note:

- This grant should not be used for the PHD work of the faculty.
- This grant cannot be used for attending or conducting conferences and workshops or for payment of registration fee.
- Books, equipment, stationery, furniture procured under the Seed Money Grant shall be the property of the Institution.
- Any intellectual property generated during the course of such a project shall be subjected to IPR policy of the institution.



Dr. M.Mohan Babu M.Tech, Ph.D
Principal

Research and Development Cell

Date: 21-08-2023

File No.: SVCET/R&D Cell/ SEED MONEY/ 2023-24/IT/003

To,

Ms. S. KOKILA,
Assitant Professor,
Department of Information Technology
SVCET, Chittoor

Sub: Letter of sanction
Dear Ms. S. KOKILA,

The Management of Sri Venkateswara College of Engineering and Technology appreciate your efforts in submitting your proposal titled "**A Hybrid Cryptosystem for D2D Communication in IoT Environment**" seeking seed grant. After thorough scrutiny, the Research Advisory Committee of the Institution has selected and recommended your proposal for the sanction of **Rs 70,000/-** to work for a period of **one** year.

This seed money grant is provided so as to enable you to undertake preliminary research work which can result either in a 'proof of concept' or 'proof of experience'. Further you are expected to apply to external funding agencies (both public and private) to take the outcomes of this project to its intended goal.

You are expected to submit progress report once in six months and also the final completion report with the utilization certificate within a month of the completion of the project.

The work done under this project shall be used only for the benefit of the institution and it will not be used or transmitted to anywhere else. The conditions for the conduct of this work will be as per the Seed Grant Policy of the institution.

Wishing you good luck



Principal

**PRINCIPAL
S.V. College of Engineering &
Technology, CHITTOOR, (A.P.)**

Payment Voucher

No. : 3824

Dated : 21-Aug-23

Particulars	Amount
Account : Research and Development New Ref Ms. S. KOKILA 70,000.00 Dr	70,000.00
Through : Cash	
On Account of : being seed money for "A Hybrid Cryptosystem for D2D Communication in IoT Environment" seeking seed grant for one year	
Amount (In words) : Indian Rupees Seventy Thousand Only	
	₹ 70,000.00

Receiver's Signature:



Authorised Signatory



Prepared by

Checked by

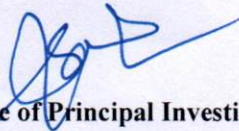
Verified by



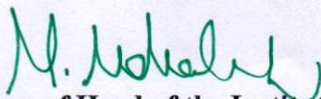
Sri Venkateswara College of Engineering & Technology (Autonomous)
R.V.S. Nagar, Tirupati Road, Chittoor – 517127. Andhra Pradesh.
(Accredited by NAAC and NBA)

UTILISATION CERTIFICATE FOR INSTITUTE FUNDED SEED GRANT

Certified that out of **Rs 70,000 (Rupees Seventy Thousand only)** of institute funded seed grant for the project titled "**A Hybrid Cryptosystem for D2D Communication in IoT Environment**" sanctioned during the Academic Year **2023 - 2024** in favour of **Mrs./Dr. S. KOKILA** from the **Department of Information Technology** dated **21/08/2023**, the entire amount has been utilized for the purpose for which it was sanctioned.


Signature of Principal Investigator
Date: 25-06-2024


ACCOUNTS OFFICER,
S.V. College of Eng & Technology,
CHITTOOR,
Signature of Accounts Officer
Date: 25-06-2024


Signature of Head of the Institution
Date: 25-06-2024
PRINCIPAL
S.V. College of Engineering &
Technology, CHITTOOR. (A.P.)



**Sri Venkateswara College of Engineering and Technology
(Autonomous)**

R.V.S. Nagar, Chittoor – 517 127

Date: 25-06-2024


PROJECT COMPLETION CERTIFICATE

This is to certify that the project titled “**A Hybrid Cryptosystem for D2D Communication in IoT Environment**” has been successfully completed under the institute-funded seed grant.

The project was sanctioned in the Academic Year **2023 – 2024** in favour of **Mrs. S. Kokila** from the **Department of Information Technology** and was carried out as per the approved objectives and guidelines. The allocated funds have been utilized effectively for the intended purpose, and all necessary reports and documentation have been submitted.


Signature of Principal Investigator

Date: 25-06-2024


Signature of Head of the Department

Date: 25-06-2024

**Head of the Department
Information Technology
Sri Venkateswara College of
Engineering & Technology (Autonomous)
Chittoor.**



Sri Venkateswara College of Engineering & Technology (Autonomous)

R.V.S. Nagar, Tirupati Road, Chittoor – 517127. Andhra Pradesh.

(Accredited by NAAC and NBA)

Project Completion Report

1. Project Title: A Hybrid Cryptosystem for D2D Communication in IoT Environment

2. Principal Investigator (PI) Details: Mrs. S. Kokila

3. Department: Information Technology

4. Funding Source and Sanction Details:

- **Funding Source:** Institute Funded Seed Grant
- **Sanction Date:** 21st August 2023
- **Grant Amount:** Rs. 70,000/-
- **Academic Year:** 2023-2024

5. Project Duration: From 21-08-2023 To 25-06-2024

6. Objective of the Project: This research aims to develop a hybrid cryptosystem to enhance the security of Device-to-Device (D2D) communication in IoT environments. The proposed solution combines symmetric and asymmetric encryption techniques to achieve improved data confidentiality, integrity, and authentication while maintaining performance efficiency.

7. Scope and Significance: IoT ecosystems face heightened security risks due to resource-constrained devices, decentralized architecture, and constant data exchange. This research addresses these concerns by:

- Designing a hybrid cryptosystem that leverages the strengths of symmetric and asymmetric encryption methods.
- Ensuring secure D2D communication across diverse IoT devices in smart homes, healthcare, and industrial environments.
- Improving resistance against man-in-the-middle (MITM), replay, and eavesdropping attacks. The proposed solution aims to balance robust security with minimal computational overhead, making it suitable for resource-limited IoT devices.

8. Methodology and Implementation:

1. System Architecture Design:

- Designing a hybrid cryptosystem integrating AES (Advanced Encryption Standard) for fast data encryption and RSA (Rivest-Shamir-Adleman) for secure key exchange.

2. **Key Management Strategy:**

- Implementing a secure key distribution mechanism using RSA to establish shared session keys.

3. **Encryption and Decryption Process:**

- Encrypting data with AES for fast and efficient processing.
- Encrypting AES keys using RSA before transmitting them between devices.

4. **Authentication Mechanism:**

- Integrating digital signatures to authenticate device identities and verify data integrity.

5. **Performance Optimization:**

- Employing lightweight cryptographic techniques to minimize energy consumption and improve processing speed.

6. **Testing and Evaluation:**

- Evaluating the cryptosystem's performance in simulated IoT environments, measuring encryption speed, computational overhead, and security robustness.

9. **Work Completed:** Yes

10. **Key Findings and Results:**

- The hybrid cryptosystem successfully achieved secure D2D communication while maintaining low latency and minimal resource consumption.
- AES encryption ensured fast data transmission, while RSA provided robust key protection.
- The system effectively mitigated common IoT security threats, including unauthorized access and data tampering.
- Experimental results demonstrated improved performance compared to traditional encryption methods in IoT environments.

11. **Outcomes and Deliverables:**

- A hybrid cryptosystem framework for secure D2D communication in IoT devices.
- An optimized key management strategy for resource-constrained environments.
- Performance evaluation metrics showcasing improved security and efficiency.
- Research documentation for potential deployment in real-world IoT systems.

12. **Challenges Faced (if any) and Solutions:**

- **Resource Constraints in IoT Devices:** Limited CPU, memory, and power in IoT nodes hinder complex encryption processes.
Solution: Use lightweight cryptographic algorithms (e.g., ECC, ChaCha20) and optimize code for minimal resource consumption.
- **Key Management Issues:** Securely distributing and updating encryption keys in a dynamic IoT environment is challenging.
Solution: Implement **Elliptic Curve Diffie-Hellman (ECDH)** for efficient key exchange and **Ephemeral Key Generation** to enhance security.

- **Latency in Encryption/Decryption:** Complex hybrid encryption schemes may increase communication delays.
Solution: Use **asymmetric encryption** only for initial key exchange and rely on **symmetric encryption** (e.g., AES) for fast data transmission.
- **Vulnerability to Attacks:** IoT networks are prone to eavesdropping, man-in-the-middle attacks, and data breaches.
Solution: Integrate **Perfect Forward Secrecy (PFS)** and **Mutual Authentication** mechanisms.
- **Scalability in Large Networks:** Expanding secure communication across multiple IoT nodes can be complex.
Solution: Implement **cluster-based key management** and efficient routing protocols for scalable security.

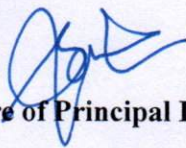
13. Utilization of Funds:

- **OpenSSL:** For implementing RSA, AES, and hybrid encryption schemes.
- **LibSodium:** Lightweight and secure encryption library ideal for IoT environments.
- **NS3 (Network Simulator 3):** For simulating D2D communication scenarios in IoT.
- **Wireshark:** For analyzing encrypted communication packets.

14. Conclusion and Recommendations:

The developed hybrid cryptosystem effectively strengthens IoT device security by combining the speed of symmetric encryption with the robust protection of asymmetric encryption. Key recommendations for future work include:

- Expanding the cryptosystem to support large-scale IoT networks with dynamic device connectivity.
- Enhancing the system's adaptability to emerging cryptographic threats.
- Integrating machine learning techniques to dynamically adjust encryption parameters for improved performance.



Signature of Principal Investigator

Date: 25-06-2024



Signature of Head of the Department

Date: 25-06-2024
 Head of the Department
 Information Technology
 Sri Venkateswara College of
 Engineering & Technology (Autonomous)
 Chittoor.