



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423

 9940 572 462

 6381 907 438

 ijirset@gmail.com

 www.ijirset.com

TTP Aided Secure Computation

Vishnukumar M, P. Prema

Student, Department of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India

Assistant Professor, Department of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India

ABSTRACT: Information data hiding is a mechanism which ensures that the presence of the secret data remains undetected. Two types of data hiding techniques are most popular, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. In the era of multimedia and internet there is need of reducing time for transmission. The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. Conventional n out of n visual cryptography scheme is used to convert a single image into n shares. LSB method is used for this purpose. Now the image is splitted into shares. Each share is encrypted using XOR method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work.

I. INTRODUCTION

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. There for the SS scheme is one of the most fundamental technologies to realize secure access control. A typical example of secret sharing schemes is a (k, n) -threshold secret sharing scheme. In (k, n) -threshold secret sharing schemes, a secret is encrypted into n shares in such a way that any k or more shares can be employed to reconstruct the secret, while no $k - 1$ or less shares leak any information about the secret. In the ordinary secret sharing schemes, secrets and shares are both numerical data and their encryption and decryption is performed by computers. In contrast, there exist secret sharing schemes whose decryption do not require any numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme is an example of such secret sharing schemes. The schemes encrypt a visual secret into visual shares so that humans can recover the visual secret with their eyes by superposing a qualified set of visual shares printed on transparencies.

II. EXISTING SYSTEM

RHD-EI allows a server to embed additional message into an encrypted image uploaded by the content owner, and guarantees that the original content can be losslessly recovered after decryption on the recipient side. The proposed secret sharing based model with multiple data-hiders is comprised of three phases: the image encryption phase, the data hiding phase, and the data extraction and image recovery phase. Different from previous methods that only involve single data hider, the proposed method involves multiple data-hiders. In this project, the original image is converted into multiple encrypted images of the same size as the original image, and the encrypted images are distributed to multiple different data-hiders for data hiding.

III. PROPOSED SYSTEM

The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This project is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. Text message was created by sender and hidden within selected cover image file. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. The text is typed and hidden in an image.

3.1 BASIC WORKING

In Trusted Third Party (TTP) aided secure computation, the focus is on enabling secure computations among multiple parties with the assistance of a trusted third party. This approach addresses the challenge of securely processing data while maintaining privacy and confidentiality. Parties involved in the computation agree on the protocol and the trusted third party (TTP) that will facilitate the computation. Each party may hold private data that needs to be processed collectively while ensuring individual privacy. Each party privately shares their inputs with the TTP. This ensures that no party directly exposes their input to others, maintaining confidentiality. The TTP performs the agreed-upon computation using the inputs provided by the parties. The computation could involve operations like addition, multiplication, or more complex algorithms depending on the agreed protocol. Once the computation is complete, the TTP shares the computed result or outputs with the parties involved. The result is typically in an encrypted form to prevent unauthorized access or tampering during transmission. After receiving the results, parties can decrypt and interpret the output as per the application's requirements. The TTP's role often extends to verifying the integrity of the computation to ensure all parties agree on the correctness of the result.

3.2 DESIGN METHODOLOGY

Designing a methodology for Trusted Third Party (TTP) aided secure computation involves several critical considerations to ensure both security and efficiency in collaborative data processing scenarios. The first step is to choose an appropriate secure computation protocol that aligns with the specific requirements of the application. Protocols like Secure Multi-Party Computation (MPC) or Homomorphic Encryption (HE) are commonly used. These protocols determine how inputs are processed, how computations are performed securely, and how outputs are generated without exposing private data. Define the role of the Trusted Third Party (TTP) clearly. The TTP could act as a facilitator, performing computations, or verifying results. It's essential to select a TTP that all parties involved trust and ensure it has the capability to securely handle the data and computations. Implement robust security measures to protect data during transmission and computation. This includes encryption of data both in transit and at rest, authentication mechanisms to verify identities of parties and the TTP, and ensuring compliance with relevant data protection regulations. Utilize techniques such as data anonymization, differential privacy, or zero-knowledge proofs to enhance privacy protections. These techniques help prevent unauthorized access or inference of sensitive information during the computation process.

IV. ER DIAGRAM

Creating an Entity-Relationship (ER) diagram for Trusted Third Party (TTP) aided secure computation involves illustrating the entities involved, their relationships, and the attributes that describe them. Here's a conceptual ER diagram for such a system. Data Owners are entities that possess private data inputs which they wish to process securely. Each Data Owner is identified uniquely within the system and can contribute multiple data inputs for computation. **Data Consumers** are entities interested in obtaining computed results based on the inputs provided by Data Owners. They interact with the TTP to access these results securely. Trusted Third Party (TTP) acts as an intermediary or facilitator in the secure computation process. It manages the interactions between Data Owners and Data Consumers, ensuring that computations are performed securely while maintaining confidentiality and privacy. Each Data Owner interacts with the TTP to securely submit their data inputs. This relationship is typically one-to-many, as the TTP can handle inputs from multiple Data Owners simultaneously. Similarly, Data Consumers interact with the TTP to receive computed results securely. This relationship is also one-to-many, allowing the TTP to serve multiple Data Consumers based on their computation requests. The TTP utilizes a specific Secure Computation Protocol (e.g., MPC, Homomorphic Encryption) to perform computations securely. This relationship is one-to-one, indicating that each TTP instance employs a single type of protocol.

The basic architect diagram is given below:

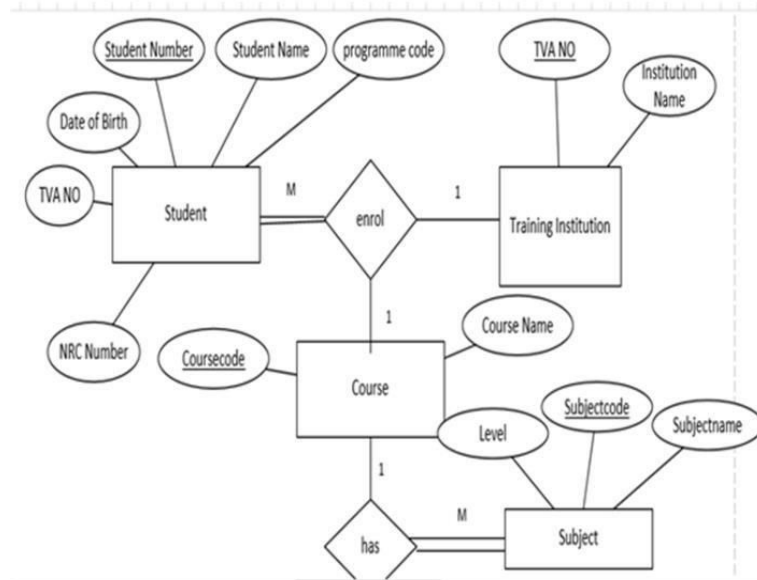


Fig-1:ER Diagram

4.1 DATA FLOW DIAGRAM

A Data Flow Diagram (DFD) is a visual representation used in systems analysis and design to illustrate the flow of data within a system. When applied to aided secure computation, such as Trusted Third Party (TTP) scenarios, DFDs play a crucial role in depicting how sensitive data is processed securely. Here’s how a DFD can aid in understanding and implementing secure computation with TTP. A Data Flow Diagram aids in visualizing and designing secure computation with a Trusted Third Party by illustrating data flows, processing steps, and security measures. It provides a clear roadmap for implementing and ensuring the confidentiality, integrity, and availability of sensitive data throughout the computation process.

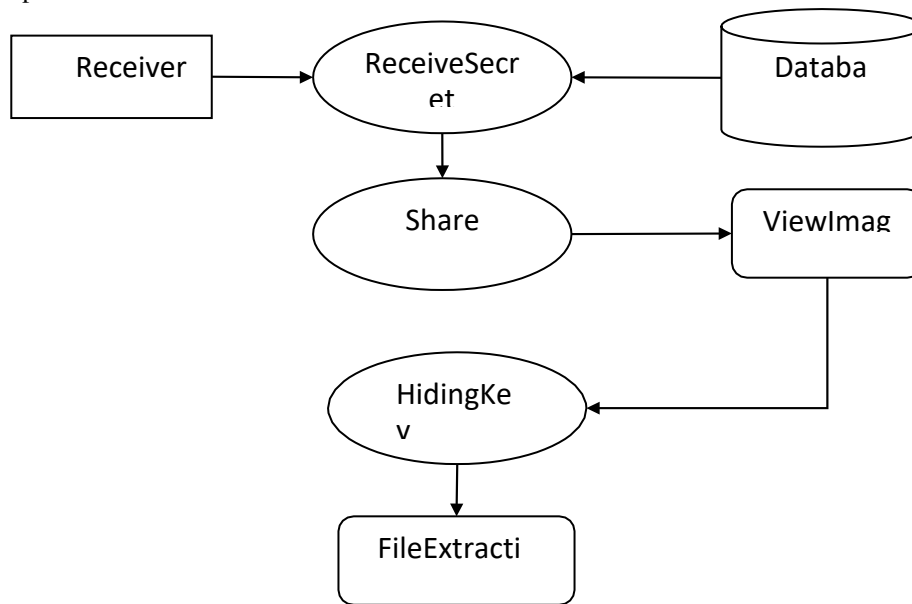


Fig-2:Data Flow Diagram

V. IMPLEMENTATION

WAMP is the most popular PHP development environment which binds My SQL data base with PHP engine. WAMP is a completely free, easy to install Apache distribution containing Maria DB, PHP and Perl. The WAMP open source package has been setup to be incredibly easy to install and to use. WAMP is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, Maria DB database, and interpreters for scripts written in the PHP and Perl programming languages. WAMP is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing and deployment purposes. Everything needed to setup a web server application (Apache), database (Maria DB) and scripting language(PHP)-is included in an extractable file. WAMP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as KAMPP, it makes transitioning from a local test server to a live server extremely easy as well.

VI. RESULTS

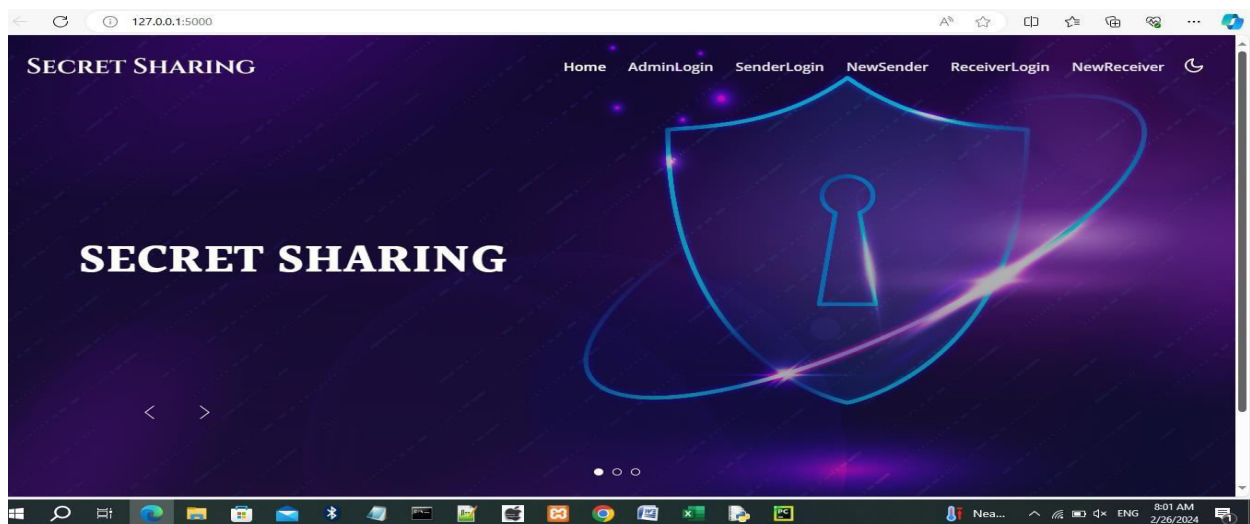


Fig-3: Home page

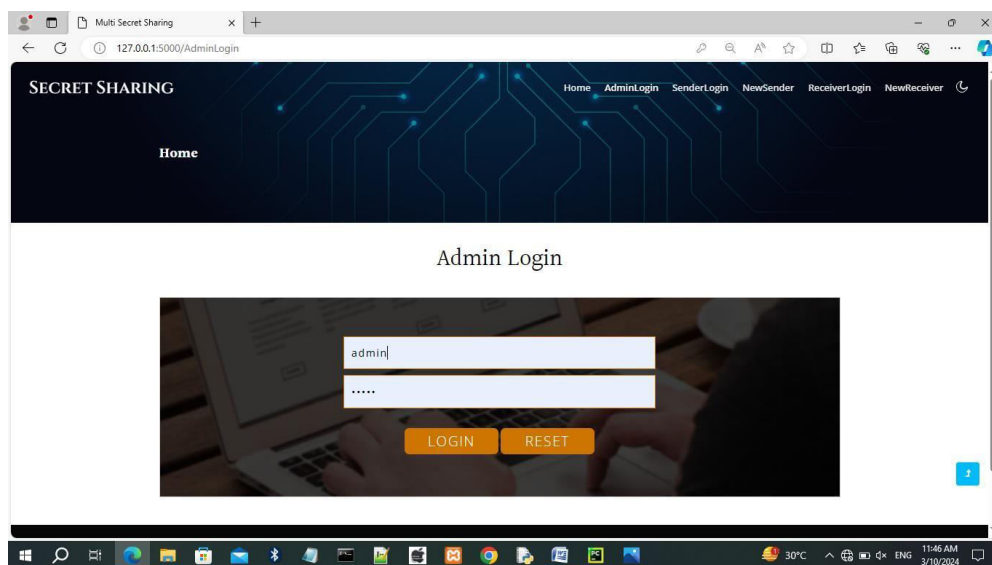


Fig-4: Admin Login

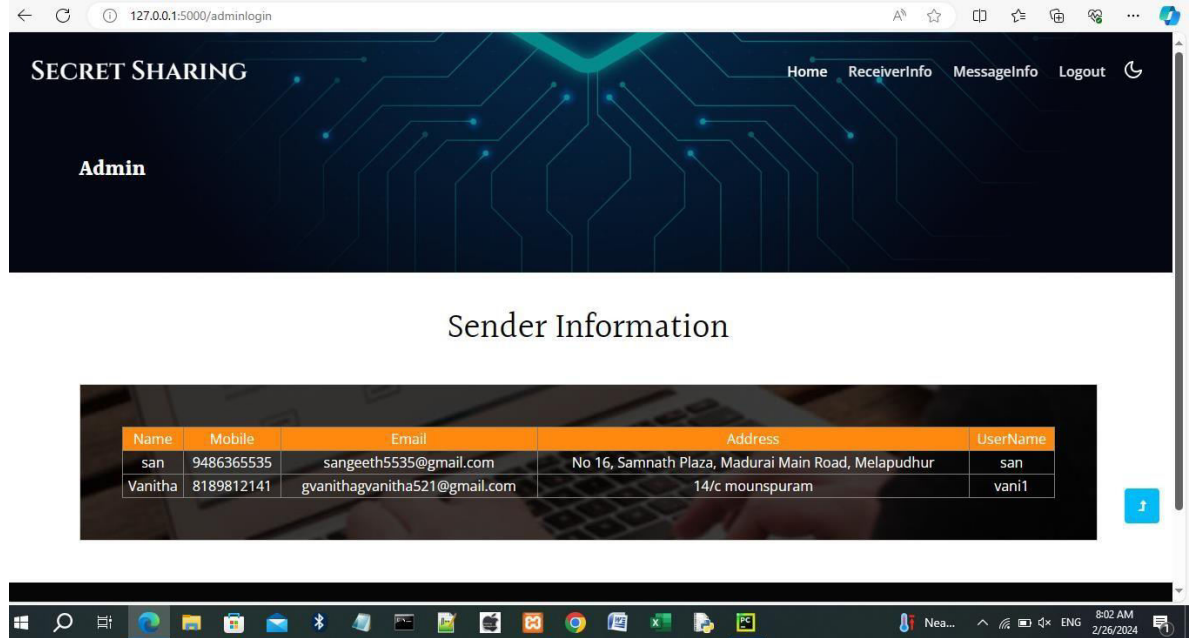
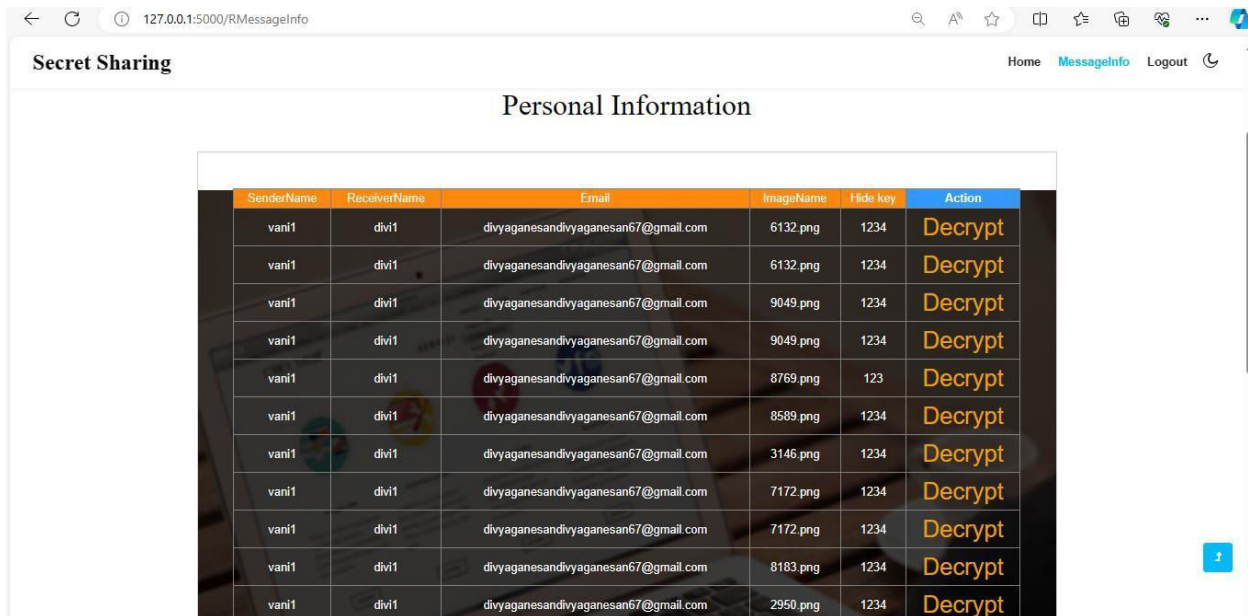


Fig-5: Sender Information



Fig-6: Receiver Information



SenderName	ReceiverName	Email	ImageName	Hide key	Action
vani1	divi1	divyaganesandivyaganesan67@gmail.com	6132.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	6132.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	9049.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	9049.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	8769.png	123	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	8589.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	3146.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	7172.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	7172.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	8183.png	1234	Decrypt
vani1	divi1	divyaganesandivyaganesan67@gmail.com	2950.png	1234	Decrypt

Fig-7: Personal Information

VII. FUTURE SCOPE

Authentication has to further improve in future. Concentrate on noise level reduction during image split and merge. Also focus on test with other share generation and encryption algorithm to identify the performance of difference cryptographic strategy. This is considered as the future work of the proposed project. In future iterations, enhancing authentication protocols with multi-factor authentication (MFA) and robust session management will bolster system security. Focus on refining image processing algorithms to reduce noise during image splitting and merging processes, preserving image quality. Exploring alternative cryptographic algorithms and conducting rigorous testing will optimize encryption strategies, balancing speed and security. Emphasizing secure key management practices and access controls will fortify data protection measures. Additionally, integrating anomaly detection mechanisms can enhance threat detection capabilities, ensuring proactive security measures. Continuous evaluation and adaptation of these enhancements will contribute to a silent and effective system.

VIII. CONCLUSION

This project describes how a secret image is securely communicated from source to destination. The sender has to select the image that should be sent secretly to the receiver. The secret image is splitted into “n” number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image. The confirmation, outfitted with the thought behind the strategy guarantees that an enemy can't alter the last picture without messing with the previous, which makes its security analysis less difficult and more efficient.

REFERENCES

1. Abdullah, Dakhaz Mustafa, Siddeeq Y. Ameen, Naaman Omar, Azar Abid Salih, Dindar Mikael Ahmed, Shakir Fattah Kak, Hajar Maseeh Yasin, Ibrahim Mohammed Ibrahim, Awder Mohammed Ahmed, and Zryan Najat Rashid. "Secure data transfer over internet using image steganography." Asian Journal of Research in Computer Science(2021):33-52.
2. Al-Shaarani, Faiza, and Adnan Gutub. "Securing matrix counting-based secret-sharing involving crypto steganography." Journal of King Saud University-Computer and Information Sciences34,no.9(2022):6909-6924.
3. Huang, Kai, XimengLiu, ShaojingFu, DekeGuo, and MingXu. "Alightweightprivacy-preserving CNN feature

extraction framework for mobile sensing. "IEEE Transactions on Dependable and Secure Computing 18,no.3(2019):1441-1455.

4. Ibrahim, Dyala R., Je SenTeh, and Rosni Abdullah. "An overview of visual cryptography techniques." *Multimedia Tools and Applications* 80(2021):31927-31952.
5. Iwamura, Keiichi, and Ahmad Akmal Aminuddin Mohd Kamal. "Secure Computation by Secret Sharing using Input Encrypted with Random Number." *InSECRYPT*, pp.540-547.2021.
6. Kamal, Ahmad Akmal Aminuddin Mohd, and Keiichi Iwamura. "Searchable encryption using secret sharing scheme that realizes direct search of encrypted documents and disjunctive search of multiple keywords." *Journal of Information Security and Applications* 59(2021):102824.
7. Kamal, Ahmad Akmal Aminuddin Mohd, and Keiichi Iwamura. "(Server-Aided) Two-Party Multiplication of Encrypted Shares Using (k, n) Threshold Secret Sharing With $N \geq k$ Servers." *IEEE Access* 9(2021):113117-113129.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details