International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

Encryption of Broadcast with Dealership

Akhila Thejaswi R [1], Swathi [2], Ushakiran S [3], Vishmitha [4], Yakshitha H [5]

[1]*Assistant Professor, Dept. of Information Science Engineering, Sahyadri College of Engineering and Management, Karnataka, India*
[2,3,4,5]*Student, Dept. of Information Science Engineering, Sahyadri College of Engineering and Management, Karnataka, India*

Abstract – *Pay TV, or also called as the subscription-based television service, provides a procedure to enable the subscribers to view the broadcast encrypted channels that are distributed by the TV Broadcaster. Recently, the scheme of Pay TV incorporates the concept of "Dealership". The concept "Dealership" is not indicated as a trusted third party, but it acts as an entity which mediates between the Broadcaster and the Subscriber during the transmission of channels. In this paper, the Broadcast Encryption with Dealership (BED) scheme is introduced. This concept is applicable to many practical broadcast services, such as television service based on the subscription. Particularly, the new scheme allows the Dealer to purchase some channels from the Broadcaster and it will allow the Dealer to retail the channels to the Subscriber with modified price. Therefore, the Dealer gets benefited by having a model that provides business opportunity. In such a situation, the security factor is essential and the security necessity should be captured. The BED scheme is secured under encryption and decryption processes using RSA algorithm.*

Key Words: **Broadcast Encryption, Decryption, Dealership, Authentication, RSA algorithm.**

1. INTRODUCTION

1.1 Network Security

Security is one of the most important factors to be considered in the network. In information technology, security is nothing but the protection of digital data, accidental and malicious threats. This protection includes identification, prevention and acknowledgement to threats by using the security policies.

Network security is used to protect the access to directories and files that are stored in the network of computer against exploit, moderation, hacking and illegal access to the system. Authorized access to data in a network is managed by the network administrator.

Network security deals with considering software and physical defensive factors to guard the network system from attacks, exploit, information disclosure, illegal access, defect, alteration, destruction, or inappropriate revelation, thereby continuously monitoring network, providing a secure staging for computers, programs and user to execute their normal or interpretative actions within a secure domain. Detection the primary task is to identify observations that are different from the characteristics of rest of the data. These observations are the anomalies. The main aim is to detect real anomalies. Association analysis is used for discovering patterns that define features that are strongly associated with data. The objective is efficient extraction of interesting patterns.

The proof-of-identity that is given by computer user is compared to the files present in the database on a local operating system or within an authentication server. This process is called Authentication. If the proof of identity is successful, then process of verification is completed and the user is permitted to access data present in the database.

Authentication factors include three types:

One-Factor Authentication (1FA): One-factor authentication is a method of providing a secured access to website or network that recognizes the user appealing permit through only one sort of proof of identity. An example for one-factor authentication is verification based on password.

Two-factor authentication (2FA): Two-factor authentication is a type of authentication where we go through a process of security measure wherein we employ two-step process that is we have two layer security it can also be summed into one which is pre-dominantly known as password. An example for two-factor authentication is the withdrawal of money from ATM.

Three-Factor Authentication (3FA): In three-factor authentication user can login to the system by confirming one's biological characteristics. This

includes biometrics scope such as fingerprint, retina scans, facial recognition and voice recognition.

1.2 RSA Algorithm

RSA algorithm is used to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography because one of them can be given to everyone. The other key must be kept private.

RSA includes a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The RSA cryptosystem is the most widely-used public key cryptography algorithm.

Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using the private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using their private key and B can verify it using A's public key.

2. ARCHITECTURE OF THE PROPOSED MODEL

An architecture diagram as shown in **Fig -1** is a description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. It identifies the various parts of the system and communication among these parts. The architecture diagram illustrates the overall framework of the project, which briefly describes the operation of the system. The Broadcaster, Dealer and the Subscriber are the three major components of the Channel Distribution System. The Dealership concept allows the Dealer to buy some channels from the Broadcaster through the Channel Distribution System and it will facilitate the Dealer to resell these channels to the Subscriber with the modified rate. Hence, it offers a business opportunity model for the Dealer.

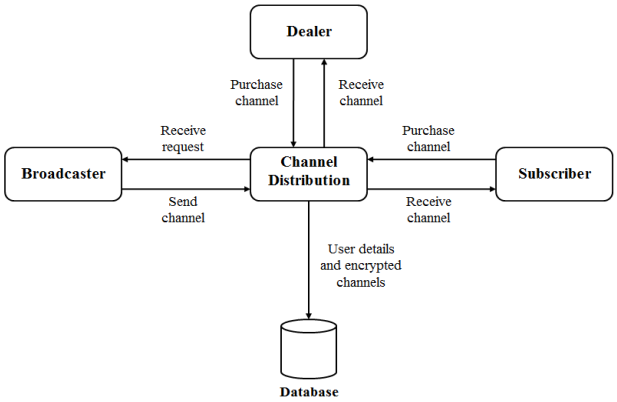

Fig -1: Architecture diagram

Modular Decomposition diagram as shown in **Fig -2**, it consists of modules, which is having different subsets of related entities for decomposing the graph. The components of a graph are connected is called as a module. The module may be the proper subset of another module similar to as components which are connected. Instead of the partition of the graph the modules performs the iterative decomposition of the graph. The communication between the broadcaster, dealer and subscriber is done through sending and receiving the channels.

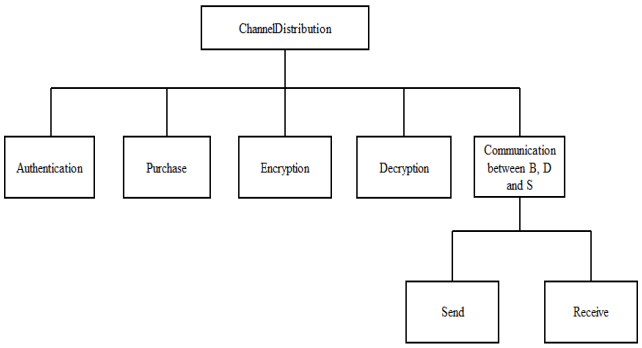

Fig -2: Modular Decomposition Diagram

4. RESULTS

The proposed algorithm is known as RSA algorithm. RSA algorithm is used to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography because one of them can be given to everyone. The other key must

be kept private. In the proposed system, initially the dealer and subscriber have to register by submitting the name, username, password, email id and adhar number and using that username and password they can login to the system. The broadcaster is given with static username and password. After the broadcaster logs in he can add the channel as shown in **Fig -3,** and he can view the channel as shown in **Fig -4**

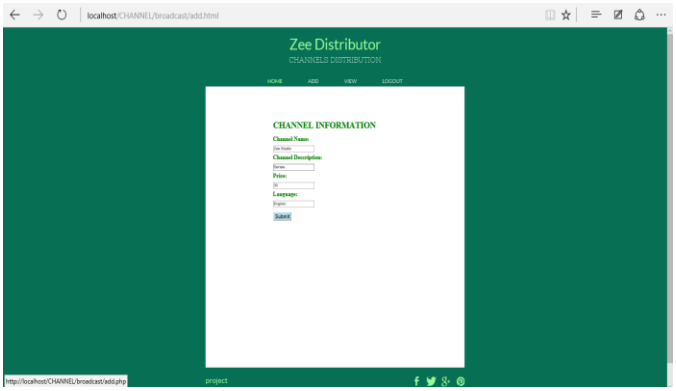

Fig -3: Adding Channel

The process of purchasing channel for Dealer and Subscriber is similar but after purchasing only Dealer can update the price of the channel. The Dealer and subscriber can purchase the channels by selecting the channel and entering the appropriate adhar number as shown in the Fig-5.

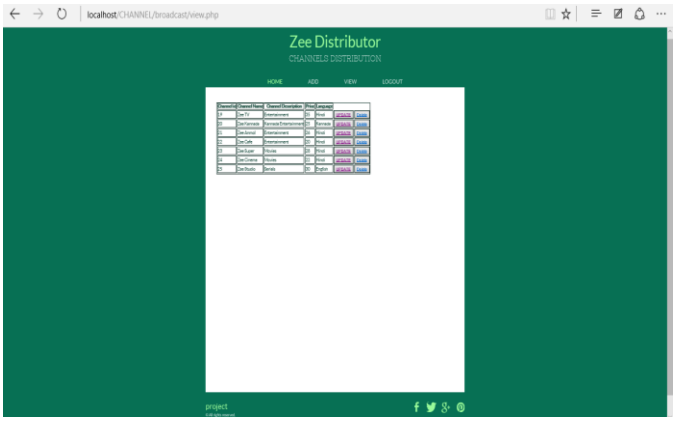

Fig -4: Viewing Channels

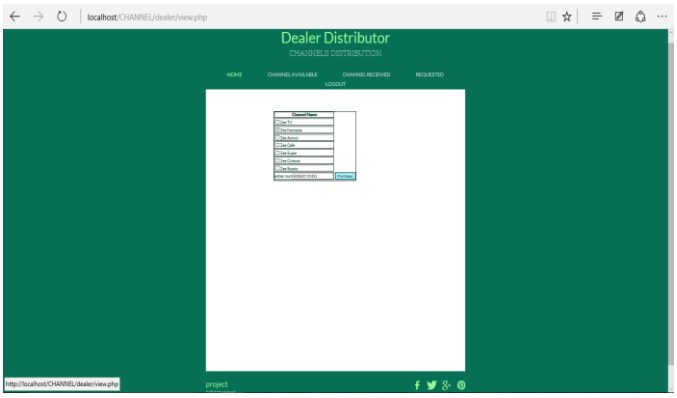

Fig -5: Purchasing Channel from Broadcaster

After the Dealer request channel from the Broadcaster, the broadcaster will get the notification by indicating the adhar number and requested channel of the dealer. The Broadcaster will check the adhar number and send the channel to appropriate dealer. Then the dealer will receive channel as shown in **Fig -6**

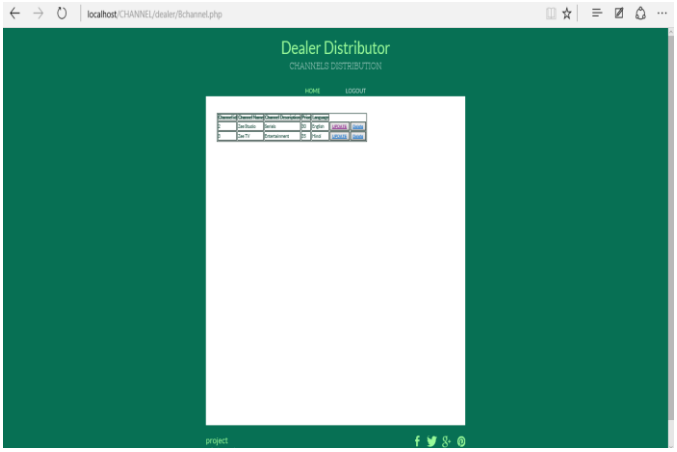

Fig -6: Received Channels

The **Fig -7** represents the performance graph of RSA encryption algorithm. This graph shows that as the channel size increases the encryption time of channel is also increases. RSA algorithm is an example for asymmetric key algorithm. Encryption and decryption are done using this algorithm which uses two different keys. One key is public and one more is private. The public key is used for encryption which is known to everyone. For decryption of cipher text private key is used which known only to the authorized persons. The public key is used to calculate the private key. The calculation of the private key is mathematically expensive.

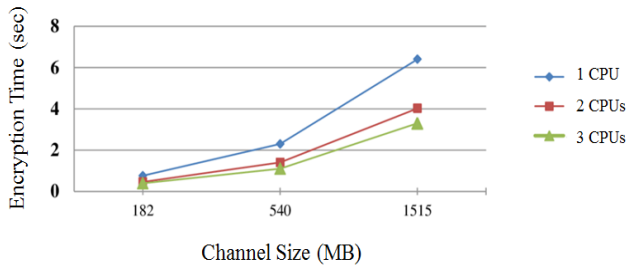

Fig -7: Graph for Channel Size and Encryption Time

The **Fig -8** represents the performance graph of RSA encryption algorithm. This graph shows that as the channel size increases the decryption time of channel is also increases.

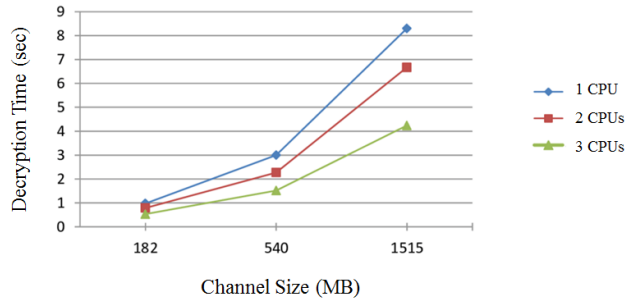

Fig -8: Graph representing passengers dead per year

3. CONCLUSIONS

The project "Encryption of Broadcast with Dealership" introduces security to the channel transmission process. Here channels are encrypted while sending and intended user can view the channels through the decryption process. RSA algorithm is used for encryption and decryption process which is fast in performance, efficient in acknowledgement and easy in execution. The possible future work is to increase the performance and to decrease the size of the cipher texts.

ACKNOWLEDGEMENT

It is with great satisfaction and euphoria that we are submitting the paper on "Encryption of Broadcast with Dealership". We are profoundly indebted to our guide, Mrs. Akhila Thejaswi R., Associate Professor, Department of Information Science & Engineering, for innumerable acts of timely advice, encouragement and we sincerely express our gratitude. We also thank her for constant encouragement and support extended throughout.
Finally, yet importantly, we express our heartfelt thanks to our family & friends for their wishes and encouragement throughout our work.

REFERENCES

[1] Clementine Gritti, Willy Susilo, Thomas Plantard, Kaitai Liang, Duncan S. Wong, "*Broadcast Encryption with Dealership*", International Journal of Information Security, ISSN(e): 1615-5262, Vol-15, Issue-03, June-2016, pp.271-283

[2] Duong-Hieu Phan, David PointCheval, Siamak F. Shahandashti, Mario Streer, "*Adaptive CCA Broadcast Encryption with Constant Size Secret Keys and Ciphertexts*", International Journal of Information Security, ISSN(e): 1615-5262, Vol-12, Issue-04, August-2013, pp. 251-265

[3] Duong-Hieu Phan, David PointCheval, Viet Cuong Trinh, "*Multi-Channel Broadcast Encryption*", International Journal on Information, Computer and Communication Security, ISBN(e): 978-1-4503-1767-2, May-2013, pp. 277-286

[4] Yevgeniy Dodis, Nelly Fazio, "*Public Key Broadcast Encryption for Stateless Receivers*", Springer Heidelberg, International Conference on Cryptology, ISBN(e):978-3-540-40410-1, Vol-2696, April-2012, pp. 61-80

[5] Craig Gentry, Brent Waters, "*Adaptive Security in Broadcast Encryption Systems*", Springer Heidelberg, International Journal on Cryptology, ISBN(e): 978-3-642-01000-2, Vol-5479, August-2009, pp. 171-188

[6] Kamalesh Acharya, Ratna Dutta, "*Secure and Efficient Construction of Broadcast Encryption with Dealership*", Springer Cham, International Journal Provable Security ISBN(e): 1615-5262, Vol-10005, November-2016, pp. 277-295