An Approach to Enhance the Distributed Adaptive Networks Security using RSA Algorithm

Shivam Sharma
Database Administrator
Newgen Software Technologies Ltd.
Noida, Uttar Pradesh

Vartika Sharma
Assistant Professor
GSSSIETW Mysuru

Abstract: **Information security in distributed systems and the use of networks for carrying data between computers is a major factor that has affected security. In this paper, we discuss security and propose security metrics issues in the context of Adaptive Distributed Systems [ADS]. A key premise of ADS is to collect detailed information based on the changes in the environment and choose efficient mechanisms (algorithms and/or encryption techniques, and secured and cost effective communication channel) for exchanging the gathered information between the targets distributed systems and the central monitoring system. Security issues in distributed systems have been solved using techniques such as cryptographic algorithms i.e. using RSA algorithm.**

Keywords: ***Adaptive distributed Systems, Encryption techniques, Cryptographic algorithms, Security metrics, and RSA algorithm.***

INTRODUCTION

A distributed system consists of a collection of autonomous Computers linked by a computer network and equipped with distributed system software. The security of data transmission is a vital problem in Distributed Systems [5]. Usually, users exchange personal sensitive information or important documents. In this case; security, integrity, authenticity and confidentiality of the exchanged data should be provided over the transmission medium. Nowadays, internet multimedia is very popular such as social networking, E-initiative (e-banking, e–commerce, e–shopping) etc. These phenomenal changes have brought about the need for tight security to data and information as a significant amount of data is exchanged every second over an unsecure channel, which may not be safe. Therefore, it is essential to protect the data from attackers [4]. Data in transit is data being accessed over the network, and therefore could be intercepted by someone else on the network or with access to the physical media the network uses. E-banking, e-commerce, e-shopping, etc., transactions over the un-trusted Communications channels are now possible because of the application of data encryption mechanisms.

Data encryption solution provides solid protection in the event of a security breach. There is an increasing use of end-to-end encryption of traffic to hide the content of transactions from the network. With encrypted traffic the users are no longer incidentally exposing their communications to the network and thereby risking exposure of their communications to unknown third parties [8].

To improve security and reliability of data being transmitted on information and communications systems; cryptography is used. Cryptography is especially useful in the cases of transmission of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over un-trusted medium like the Internet. Cryptography is the science of keeping the transmitted data secure. It provides data encryption for secure communication. The encryption process is applied before transmission, and the Decryption process is applied after receiving the encrypted data. The information hiding Process is applied before transmission and the extraction process is applied after receiving.

LITERATURE REVIEW

Adaptive Distributed Systems (ADSs) are distributed systems that can evolve their behaviors based on changes in their environments. A mainstay with adaptation of distributed systems is that in order to detect changes, information must be collected by monitoring the system and its environment. Contrariwise, the impact of implementation of security mechanism on the adaptation of distributed system is also determined. There should be security against the unauthorized access of the network and the information transmitted over the networks.

There are many researches done and are being done on the various security issues in distributed adaptive networks. The most of the literature works which are considered here discusses about the various security metrics involved in a secure distributed adaptive network.

The various research works on several cryptographic algorithms are also explored. Those works elucidate the different kinds of cryptographic algorithms like, Symmetric and Asymmetric cryptography. They also unfold the algorithms that comes under these types and discusses their pros and cons.

A survey on these research works gives a conclusion that RSA algorithm is best in order to secure a distributed adaptive network. It is a asymmetric algorithm having two separate

keys each for encryption and decryption making the data over network shielded from an unauthorized intruder.

[1] "Network Security with Cryptography"

In this paper, a concept to protect network and data transmission over a network is discussed. It states that data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

[2] "Secure Communication using RSA Algorithm for Network Environment"

This paper discusses that secure communication in network environment is primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and e-commerce transactions, digital signatures using public key cryptography is extensively employed. To maintain confidentiality, Digital Envelope, which is the combination of the encrypted message and signature with the encrypted symmetric key, is also used. This research paper has proposed to develop a hybrid technique using Symmetric & Asymmetric key cryptography. It will also include Message authentication code to maintain integrity of message. Therefore, proposed model will not only help to maintain confidentiality and authentication of message and user but integrity of data too.

[3] "Hybrid Cryptographic Technique using RSA algorithm and scheduling concepts"

It states that RSA algorithm is one of the most commonly used efficient cryptographic algorithms as it provides the required amount of confidentiality, data integrity and privacy.

This paper integrates the RSA Algorithm with round-robin priority scheduling scheme in order to extend the level of security and reduce the effectiveness of intrusion.

In this method the user uses the RSA algorithm and generates the encrypted messages that are sorted priority-wise and then sent. The receiver, on receiving the messages decrypts them using the RSA algorithm according to their priority. This method reduces the risk of man-in-middle attacks and timing attacks as the encrypted and decrypted messages are further jumbled based on their priority

[4] "Analysis of Different Security Issues and Attacks in Distributed System A-Review"

It states that so many people are connected to the internet to access the different resources of their use and different companies are using distributed environment to provide their services to the customers. All these activities affect the economy of the country or world. So there is a need of more secure distributed environment in which all transaction and operations can be complete successfully in a secure way. In distributed System environment it is very important to provide service at anytime, anywhere to the customers, this require proper time management of all computing and networking resources, resource allocation on time and their proper utilization. In distributed environment security is primary concern. In this paper an analysis of different security issues related to data, physical security, network security, possible distributed system attacks, has been made.

[5] "A Review on Security Issues in Distributed Systems"

This paper discusses about the development of secured and trusted distributed systems. This paper is a contribution towards the summarization of work carried out in this field as well as identifies new research lines. It states that security techniques in distributed systems are the important issues. Several elements of distributed system security are identified, like authentication, authorization, encryption and system protection. Several approaches about security aspects in distributed systems have been discussed, like authentication based approaches, development of trust based models, access control based approaches, etc. A summarization of these issues is given in conclusion section. Apart from this, many research lines about secure distributed systems are discussed.

[6] "Data Security Using Private Key Encryption System Based on Arithmetic Coding"

This paper discusses about the problems faced by today's communicators and it states that not only security but also the speed of communication and size of content is important. In the present paper, a scheme has been proposed which uses the concept of compression and data encryption. In first phase the focus has been made on data compression and cryptography. In the next phase it emphasizes on compression cryptosystem. Finally, proposed technique has been discussed which used the concept of data compression and encryption. In this first data is compressed to reduce the size of the data and increase the data transfer rate. Thereafter compress data is encrypted to provide security. Hence the proposed technique of this paper is effective.

[7] "Implementation of Security in Distributed Systems – A Comparative Study"

This paper presents a comparative study of distributed systems and the security issues associated with those systems. Four commonly used distributed systems were considered for detailed analysis in terms of technologies involved, security issues faced by them and solution proposed to circumvent those issues. Finally the security issues and the solutions were summarized and compared with each other. It also states that security becomes more prominent when the systems have been distributed across over multiple geographic locations. Each type of distributed system has its own peculiar security requirements.

PROPOSED METHOD

The proposed system uses Adaptive systems which makes a wider variety of actions possible to compensate for the changes in the environment. In this system, security issues

are addressed, in particular security metrics, in the context of ADSs and an approach is proposed towards assessing the impact of monitoring for adaptation on effectiveness of security mechanisms.

The system monitors the communication channels to obtain secure communication. It maintains information about each client. If an anonymous tries to enter into the network and tries to access the authorized client's data, he receives encrypted data. Therefore, it presents a good quality of service to the users of distributed systems.

The primary advantage of RSA public-key cryptography is increased security and convenience: private keys never need to be transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted since the same key is used for encryption and decryption.

Security is ensured in two ways: In this encryption the two parties don't need to have already shared their secret in order to communicate using encryption and that both authentication and non-repudiation are possible. (Authentication means that you can encrypt the message with my public key and only I can decrypt it with my private key. Non-repudiation means that you can "sign" the message with your private key and I can verify that it came from you with your public key.) . Therefore, the encryption serves as a fingerprint, since only your private key could have encrypted the data.

METHODOLOGY

Many encryption algorithms are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA and ECC).

Symmetric algorithms are relatively simple and quick, but if third parties intercept the key they can decrypt the messages. To overcome this drawback asymmetric encryption comes into picture.

Cryptography encrypts the message and transmits it; anyone can view the encrypted message, but is very difficult to be understood, especially if it has been encrypted with a strong cryptographic algorithm such as RSA cryptographic algorithm. It is an asymmetric cryptographic algorithm.

In RSA cryptography, **RSA** stands for Ron Rivest, Adi Shamir and Leonard Adleman is an algorithm used by modern computers to encrypt and decrypt messages. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key [9]. The prime factors must be kept secret. Anyone can use the public key to encrypt a message. The RSA algorithm involves three steps:

- Key generation
- Encryption and
- Decryption.

Key generation

RSA involves a **public key** and a **private key.** The public key can be known by everyone and is used for encrypting messages. The private key is used to decrypt the message which is encrypted with the public key.

The keys for the RSA algorithm are generated the following way:

 Choose two distinct prime numbers p and q, the integers p and q should be chosen at random.

 Compute $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

 Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$, where φ is Euler's totient function. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e. e and $\varphi(n)$ are co-prime. e is released as the public key exponent. Determine d as $d-1 \equiv e \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$). This is more clearly stated as solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$ d is kept as the private key exponent. By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

 The public key consists of the modulus n and the public (or encryption) exponent e.

 The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d [9].

Encryption

Consider an analogy where two people Alice and Bob are communicating. Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. He then computes the cipher text c corresponding to

c=m^e(mod m)

Bob then transmits c to Alice.

Decryption

Alice can recover m from c by using her private key exponent d via computing

m=c^d(mod n).

Given m, she can recover the original message M by reversing the padding scheme.

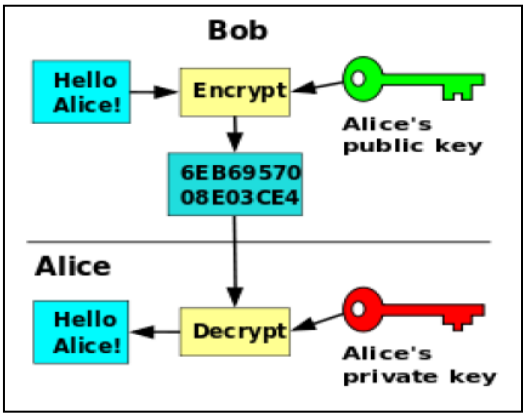

Fig 1: RSA Encryption and Decryption

CONCLUSIONS

In this study, we did a comprehensive review of public and private key cryptosystem called RSA algorithm. RSA encrypts message with strongly secure key which is known only by sending and receiving end, is a significant aspect to acquire robust security. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity.

The system monitors the communication channels to obtain secure communication. It maintains information about each client.

In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds.

REFERENCES

[1]. Mukund R.Joshi, Renuka Avinash Karkale "Network security with Cryptography", Vol. 4, January 2015.
[2]. Amrita Jain, Vivek Kapoor. "Secure Communication using RSA Algorithm for Network Environment", International Journal of Computer Applications (0975 – 8887) Volume 118 – No. 7, May 2015.
[3]. Meenakshi Shankar Akshaya.P, "Hybrid Cryptographic Technique using RSA algorithm and Scheduling concepts", International Journal of Network Security and its Application, Vol. 6, Nov 2014.
[4]. Manoj Kumar, Nikhil Agrawal, "Analysis of Different Security Issues and Attacks in Distributed System", International Journal of Advanced Research in Computer Science and Software Engineering, April 2013.
[5]. Vijay Prakash, Manuj Darbari, "A Review on Security Issues in Distributed Systems", International Journal of Scientific and Engineering Research, Vol. 3, Sept. 2012.
[6]. Ajit Singh and Rimple Gilhotra, "Data Security Using Private Key Encryption System Based on Arithmetic Coding", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011
[7]. Mohamed Firdhous, "Implementation of Security in Distributed Systems – A Comparative Study", International Journal of Computer Information Systems, Vol. 2, No. 2, 2011.
[8]. Oleksandr Bodriagov, Sonja Buchegger, "Encryption for Peer-to-Peer Social Networks", IEEE Third International Conference on Social Computing, 2011.
[9]. Chandra M. Kota et al., "Implementation of the RSA algorithm and its cryptanalysis," In proceedings of the 2002 ASEE Gulf-Southwest Annual Conference, March 20 – 22, 2002.
[10]. Erfaneh Noorouzil, "A New Digital Signature Algorithm", International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011.
[11]. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Anaysis", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011
[12]. Manjunath Kotari, Dr.Niranjan N, "Monitoring and its Impacts over Distributed Systems and Possible Solutions", International Journal of Computer Science and Mobile Computing, Vol. 2, June 2013.
[13]. Simon Blake Wilson, "Key agreement protocols and their security analysis," 9-sep-1997.
[14]. Prince Oghenekaro Asagba, Enoch O.Nwachukwu, "A Review of RSA Cryptosystems and Cryptographic Protocols", West African Journal of Industrial & academic researchVol.10 No.1. April, 2014.
[15]. Pratap Chandra Mandal, " Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012.
[16]. Rajdeep Bhanot, Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and its Applications, Vol. 9, 2015.
[17]. Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013
[18]. Akankasha Bali, Dr.Shailendra Narayan Singh,"A Review on Network Security related to Wireless Sensor network", International Journal of Advanced research in Computer Science and Software Engineering, Vol.5,March 2015.