IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Secure Text Encryption in Intranet Using Elliptic Curve Cryptography

Arpana Kumari[1*], Vivek Kapoor[2]

[1,2] Dept. of Information Technology, Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, India

[*]*Corresponding Author: arpanakumariit07@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i6.981984 | Available online at: www.ijcseonline.org

Accepted: 14/Jun/2019, Published: 30/Jun/2019

Abstract— The intranet-based applications are safe and in-house applications hosted inside the internal network. Internet applications need internet to process client requests from the browser to web server instead they only need internal communication with an internal dedicated server. Most companies like to deploy such applications to keep their sensitive data inside the network. Army organizations are best examples instead to store data at the remote server through the internet, they prefer to use a local server with the intranet. This work observes the need for security inside intranet-based applications. It implies designing intranet application by mitigating issues evolved in existing work. This work proposed to use of Elliptic Curve Cryptography and RC6 algorithms to keep data safe and secure inside the intranet using double layer security mechanism. The complete work will be implemented using Java technology and a small application will be created to evaluate the performance of the proposed solution.

Keywords— Intranet application, Elliptic curve cryptography, Cryptographic technique, Data security.

I. INTRODUCTION

Intranet network is used basically by organizations in an individual manner. It is an application used over an internal network. This improves productivity and efficiency. Every company has its intranet network, which is operated by a member of that company. One or more gateways are used for connection outside the internet.

In existing work, encrypted data is searched using indexing. The approach used works on receiving a public key and shares it with the user. Private Key is used to encrypt data. The author applied fully homomorphic encryption for multiple sub-user. It prevents the confidentiality and integrity of the original data. Data outsourcing is done, and data accessing is easy. Multiple sub-users are formed by the user having sub-user with a data subset. The author concluded that it is a better technique than RSA for the security of data.

The Section I contains the introduction of intranet and encryption technique, Section II contain the related work of implemented an approach using ECC and RSA with a new mapping technique to map plaintext on elliptic curves, Section III contains methodology of the proposed work using block diagram, Section IV contain result and discussion, section V contains conclusion and future work.

II. RELATED WORK

Keerthi K et al. In [1] implemented an approach using ECC and RSA with a new mapping technique to map plaintext on elliptic curves.

Entities in intranet application should be trusted entity; if low trusted entity arises then security issues are generated. Therefore, trust relation is important, and this factor of trust is very less, this is one of the issues in security.

Many organizations or user wants their data to be stored separately from other user's data for security, but separate storage is not possible neither user knew where their data is in data center nor they are known in which data center data is located. For every individual or organization, it is not possible to store data separately, for separate storage, private cloud is required. Security problems are also the issues where conditions and situations of data confidentiality rise in system applications. Confidentiality of data is very essential for the preservation of sensitive data.

Different issues in systems are the major concern on which is focused on and reducing those operational and computational hindrances is the best thing to work on for better architecture. Data storage is a very risky part and for it, security is the biggest requirement, for storing any file security essentials are important. Some security credentials are necessary for data communications because of data sniffing while transferring data from sender to receiver.

III. METHODOLOGY

Proposed work describes the working of complete work where the key is generated and then encryption and decryption is performed on chunk data for achieving confidentiality for encryption and decryption.
Packaging includes system overview and block architecture.
A. Key Generation:
System architecture explained through diagram is shown in figure 1, 2, 3, 4, 5

Word tokenization with calculating Term frequency:

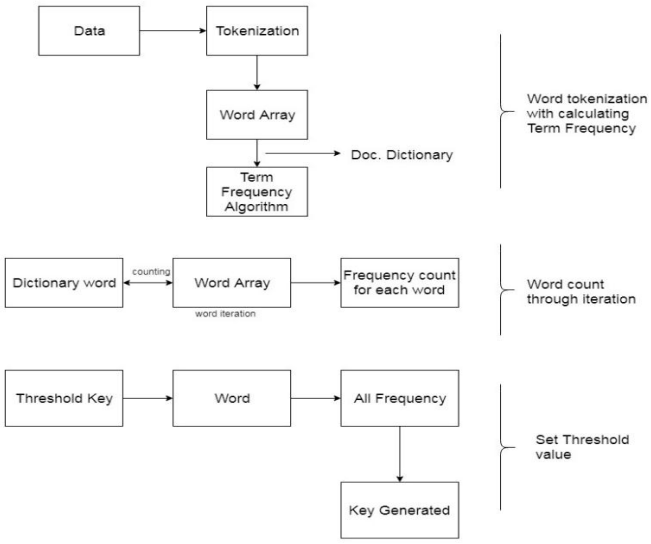
- Data will be taken as input.
- Then input data will be tokenized with no limitation / no cleaning.
- Using Term Frequency Algorithm, it will calculate the frequency of word occurrence.

Word count through iteration:

- It picks one word from the list & makes a list called Doc Dictionary.
-
- Word count from dictionary through word iteration with counting frequency for each word.

Set Threshold value:

- From the set threshold value, the threshold value enters a random number
- Word use about the frequency.
- Word, which is less than the frequency count, will not participate in key generation.
- At last, the key will generate.



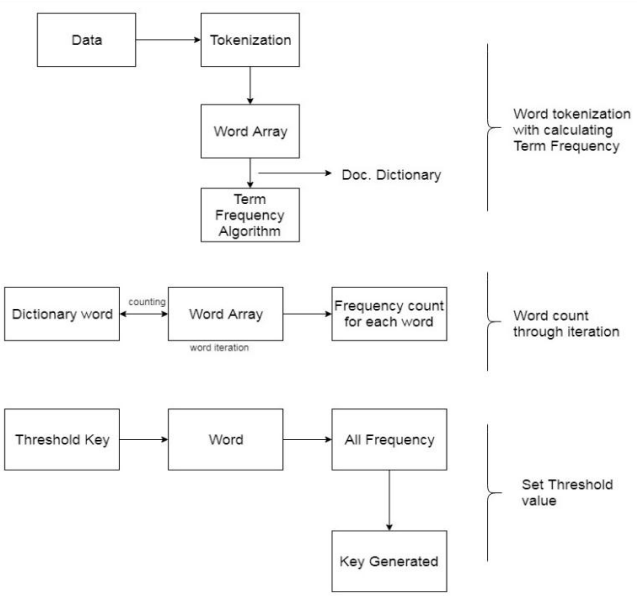


Figure 1: Key Generation

B. Cryptographic Technique
The cryptographic technique defines the encryption and decryption of data through chunks. It is done for the purpose of prevention from a replay attack.

Encryption:

- Elliptic Curve Cryptography and RC6 Algorithms has been integrated as an encryption approach. Initially, the Elliptic Curve Cryptography algorithm is used to encrypt complete plain text using receivers' public key.
- Afterward, the RC6 algorithm has been used to provide dual level security and enhance the confidentiality and privacy of the proposed solution.
- The token-based key has been used to encrypt Elliptic Curve Cryptography generated Cipher Text and provide dual level security.

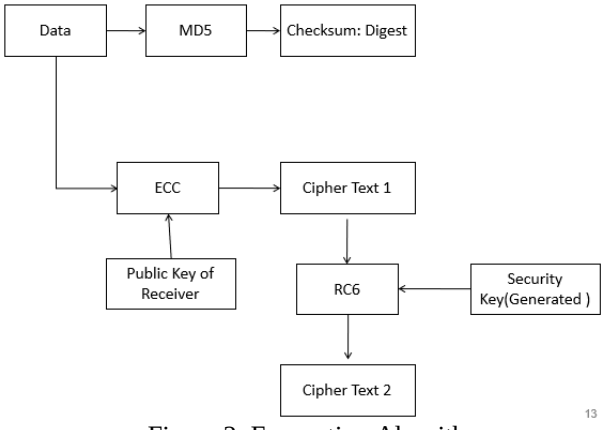


Figure 2: Encryption Algorithm

Decryption:

- Ciphered text is decrypted using the generated key.
- With decrypting, converting them into a plain text.

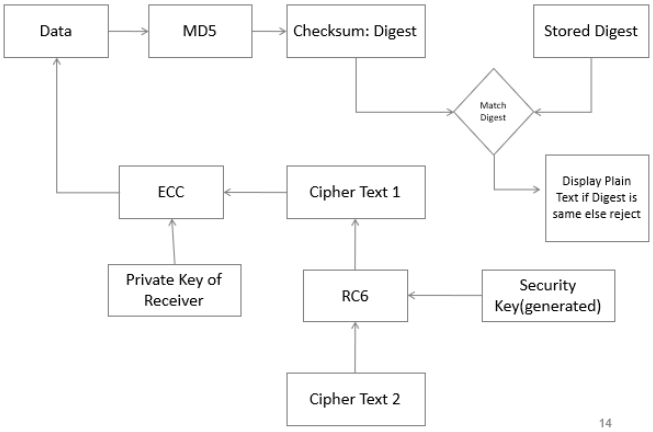


Figure 3: Decryption Algorithm

Checksum calculation:

- The checksum will be calculated with applying ECC algorithm and converting them into cipher checksum.
- Here, the size of the checksum is equal to the size of plain text.

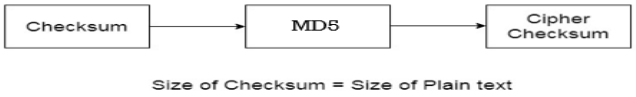


Figure 4: Checksum calculation

Checksum comparison:

- Key received will be used to decrypt and then compute the checksum.
- The checksum will be re-computing for comparison.
- If false, then reject.
- True, and then accept.

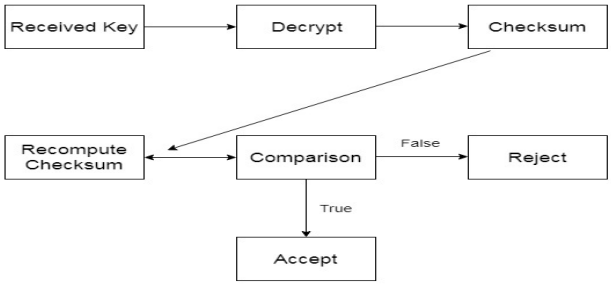


Figure 5: Comparison of Checksum

System overview:

The generated key is used to decrypt plain text by converting plain text into cipher text.

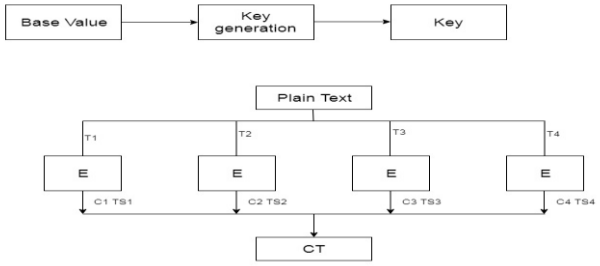


Figure 6: System overview

IV. Results and Discussion

The solution we proposed will be able to provide integrity and confidentiality as a double layer security mechanism is been applied. It will also reduce the time of encryption and decryption. To achieve this result, we use elliptic curve cryptography and RC6 algorithms.we use java technology for executing this methodology.

V. Conclusion and Future Scope

Intranet applications are becoming popular among big organizations to keep data safe and store inside an organization. In-house chatting, file transfer applications, source code repositories are an example of such applications. This work observes that Elliptic Curve Cryptography is one of the best asymmetric key-based algorithms to keep communication safe from outside fabrication or information leakage. In this paper, the solution will provide secure encryption and decryption using a checksum. Security is implemented at the end of encryption and chunk distribution. Here, the size of the checksum is equal to the size of plain text. At the initial level of analysis, the system seems to satisfy all the demand for security effectively.

Following future work is observed inside research activity

- The proposed solution should be implemented and evaluated with a well-settled organization based on computation and memory overhead.
- Proposed work can be expanded on the cloud application.
- The proposed solution can be implemented in a Hadoop environment.
- Security architecture can be used for a mobile application.

Acknowledgment

I am grateful to the Department of Information Technology, Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya University Indore for providing all conveniences to me related to my research work.

REFERENCES

[1] Keerthi K, Dr. B. Surendiran, "Elliptic Curve Cryptography for Secured Text Encryption". 2017 International Conference on circuits Power and Computing Technologies [ICCPCT], 2017 IEEE.

[2] S.M. C Vigila and Munseeswaran," Implementation of Text based cryptosystem using elliptic curve cryptography", 2009 1st International conference on advances computing, ICAC 2009, pp.82-85,2009.

[3] L. D. Singh and K. M. Singh," Implementation of Text Encryption using Elliptic Curve Cryptography", Procedia Computer Science, vol.54, no.1, pp. 73-82,2015

[4] Akshita Bhandari, Ashutosh Gupta, Debasis Das, "A framework for Data Security and Storage in Cloud Computing". International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016.

[5] Milind Mathur, Ayush Kesarwani, "Comparison between DES, 3DES, RC2, RC6, BLOWFISH, and AES". Proceedings of National Conference on New Horizons in IT – NCNHIT 2013.

[6] A Arjuna Rao, K Sujatha, A Bhavana Deepthi, L V Rajesh, "Survey paper comparing ECC with RSA, AES and Blowfish Algorithms" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5, Issue: 1, IJRITCC, January 2017.

[7] Atul Kahate "Cryptography and Network Security", Second Edition-2003, Tata McGraw Hill New Delhi, 10th reprint-2010.

[8] M. Wiesmann, F. Pedonet, A. Schiper, B. Kemmet, G. Alonso "Database Replication Techniques: a Three Parameter Classification" published in Reliable Distributed Systems, 2000. SRDS-2000. Proceedings. The 19th IEEE Symposium on at Lausanne PP. 206-215.

[9] DV Kapoor, R Yadav "A hybrid cryptography technique to support cyber security infrastructure" - Int. J. Adv. Res. Computer. Engg. Technology, 2015

[10] V. Kapoor, "A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.39-46, 2013

[11] G.L. Pavani, Ch.Ramesh, "*Secure Data Retrieval using Cipher Text Policy-Attribute Based Encryption in Hybrid Networks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.4, pp.45-48, 2017

[12] A hybrid cryptography technique for improving network security
V Kapoor, R Yadav - International Journal of Computer Applications,2016

[13] A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission 1
T Panse, V Kapoor, P Panse - 2012

Authors Profile

Arpana Kumari currently pursuing a Master of Engineering from Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya University Indore and completed a Bachelor of Engineering in 2016 from Swami Vivekanand College of Engineering, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal.

Vivek Kapoor currently working as an Assistant Professor in the Department of Information Technology, Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya University, Indore.

