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

Proposed Hybrid Cryptographic Technique To Secure Data In Web Application

Neha Gupta[1*], Vivek Kapoor[2], Jyoti Haweliya[3]

[1] Department of Information Technology, Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, India
[2] Department of Information Technology, Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, India
[3] Department of Computer Engineering , Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, India

[*]*Corresponding Author: neha.svit@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i6.971975 | Available online at: www.ijcseonline.org

Accepted: 12/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Web applications are becoming a necessary part of modern life. Security is one of the most important non-functional requirements of every solution. Early days, security and data privacy was just luxury part of software development and it was an optional requirement but nowadays it plays a critical role in daily life. This research paper has been made to observe the need for security algorithms in web application. This work observes that the current security level of existing applications and also recommend improved security solutions to enhance the security level as well performance of proposed architecture. This work recommends that ECC (asymmetric key cryptography) and Blowfish algorithm (symmetric key cryptography) can be used to achieve confidentiality during communication. It also considers the MD5 algorithm to maintain the integrity and modified Kerberos algorithm to achieve authentication. The complete work will propose a security architecture having solution to achieve confidentiality, integrity with strong authentication policy for web application development.

***Keywords*—**Web based application, RC6, ECC, Blowfish, Kerberos authentication.

I. INTRODUCTION

A Web Applications is a combination of backend and frontend utilized web browser and technology to perform the task over the internet using HTTP or HTTPS protocols. It uses a web server to run server source code and perform server end computation. A block diagram to represent complete web application architecture is shown in figure1.

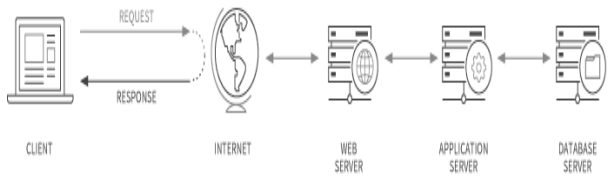


Figure 1. Block diagram of Web Application.

Here, a brief description of all necessary components used in the web application is cited below:

A. Web Browser

The User triggers requests from the web browser and send it through the internet.

B. Web Server

Web server forwards the incoming request to the appropriate application server.

C. Web Application Server

Application servers perform execution task such as queering or processing data and response to the client in the web browser.

D. Database Server

The Database server is used to store all application data and perform database related operation such as a query. The client cannot directly interact with the database server further; it always gets a request from the web server and response to the web server only.

Web applications enable the system with cross-platform functionality regardless of the software and messaging

© 2019, IJCSE All Rights Reserved

between these cross-platforms is necessary. At this point, hackers attack and break down the security. In web application Data is recognized as an important corporate asset that needs to be safeguarded from unwanted internal or external threats. Data encryption provides data protection on sensitive data but also raise computation and memory overhead on web application during large data processing. Web Application always demands low processing overhead to keep computation as fast as possible.

In [1] proposed work on Hybrid Cryptography Algorithm using RSA and AES algorithm. Researchers use AES algorithm for primary encryption which suffers with the issue of extra computation time over other symmetric key algorithms. It can be replaced by Blowfish security algorithm which is faster than AES. RSA algorithm also provides less security than ECC algorithm. ECC algorithm can provide the same level of security afforded by RSA with a large modulus and corresponding large key. Authentication and Integrity are also not achieved in [1] the proposed work. Hence, the above stated issues are the problem that is overcome in this paper using the best techniques to secure data in web applications. At the end, we will provide an architecture which will ensure confidentiality, integrity, and authenticity in web applications. The proposed methodology will give the best and fast way to secure data in web application.

The rest of the paper is organized as follows, Section I contains the introduction of web application, need of security in it and encryption techniques to secure it, Section II contain the related work of hybrid cryptographic technique in various areas, Section III explain the proposed methodology with block diagrams of system architecture, Section IV describes results and discussion, Section V concludes research work with future directions).

II. RELATED WORK

The literature survey describes the working of algorithms and techniques used in this paper and also the mitigation approach discovered, explaining the methods evolved for the improvement of basic versions.

K. M. Abdullah, E. H. Houssein, H. H. Zayed. In [1] proposed a hybrid algorithm by combining public key cryptography with symmetric cryptography. In this algorithm, author use 128 bit AES key and 2048 bit RSA key. They also use LZW compression technique to reduce the ciphertext size. This becomes easier, faster and also secure for transferring information in Wireless Sensor Network.

Milind Mathur, Ayush Kesarwani. In [2] compared various algorithms like DES, RC6, AES, and many others on several file size. By comparing algorithms we used RC6 and BLOWFISH to elaborate results for the research work.

M. Harini, K. Pushpa Gowri, C. Pavithra, M. Pradhiba Selvarani. In [3] designed a security algorithm to implement better security. The author used a hybrid solution to overcome issues of AES algorithm. They used MD5 and integrated AES and RSA algorithms to enhance security. They calculate the hash value of plain text using MD5 then encrypt calculated hash value with RSA and encrypt plain text using AES algorithm.

Jayraj Gondaliya, Jinisha Savani, Vivek Sheetal Dhaduvai, Gahangir Hossain. In [4] described cryptosystem using hybrid RSA. The complexity of the system is increased by multiplying more than two large prime number based on the RSA cryptosystem. But the Hybrid RSA algorithm takes more key generation time than RSA. It also takes a long time for encryption and decryption for the large prime.

III. METHODOLOGY

The proposed methodology describes a secure encryption process by generating the key, where the base key is used in generating the number of keys K1, K2,…,Kn. After that, it performs authentication to authenticate the client using modified Kerberos before encrypting/decrypting the data to achieve confidentiality. Then it performs encryption/decryption using ECC and BLOWFISH algorithm. It also uses MD5 to maintain the integrity of data. Below diagrams show the flow of complete work.

A. Authentication Model

To achieve authenticity modified Kerberos is used, where the user first login and Kerberos server authenticates to check credentials. If the credentials are valid then login will be successful and will redirect to home. Through this process, authentication will be achieved in the proposed work. In the proposed authentication protocol we use only one server named as Authentication Server for authentication and for generating the token instead of two servers used in Kerberos 5 protocol. The proposed authentication steps are as follows.

- The Client who wants to access the services of resource server first login to authentication server using email id and password.
- After verifying the client Authentication server generates an encrypted token (ET_K) using RC6 algorithm and send it to the client.
- The Client then sends encrypted token (ET_K) to the resource server in order to get its services.
- Resource server first decrypt the token (ET_K) send by the client then verify the token (T_K) to check whether is expired or not. If Token ($T_{K)}$ is not expired then

© 2019, IJCSE All Rights Reserved

Resource server starts providing services to client else it simply discards the token (T_K) and does not provide the services.

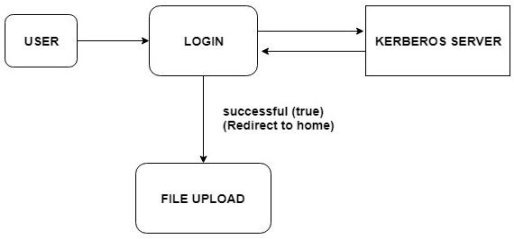


Figure 2. Block diagram of Authentication Model.

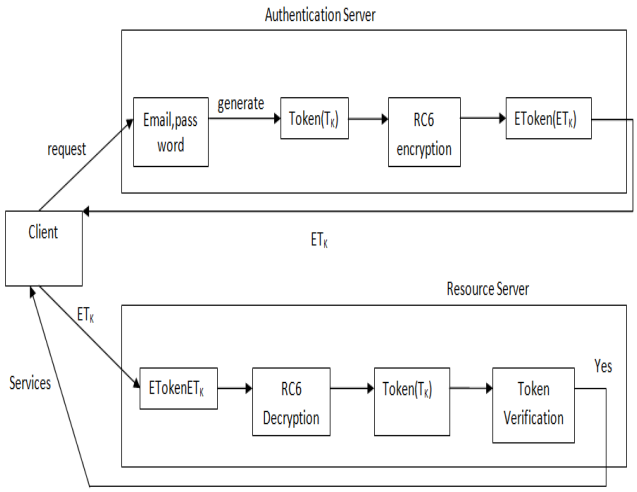


Figure 3. Authentication Protocol Architecture.

B. *Integrity calculation Model*

The File is uploading and MD5 is applied to it before encryption with MD5 generation 256 bit. The integrity of the file will be checked in this process. It will check the originality of file.

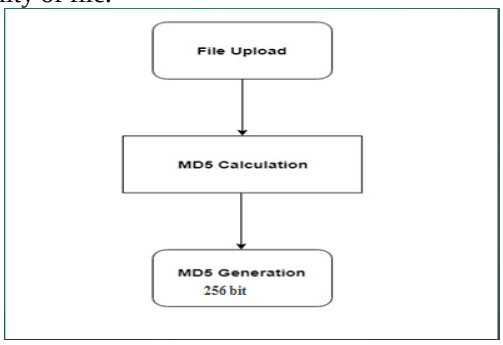


Figure 4. *Block diagram of Integrity Calculation.*

C. *Encryption Model*

Confidentiality is calculated by encrypting and decrypting a file. The encryption process will be as; firstly, the file will be taken as input and then it is divided into chunks forming chunk pool C1, C2, …., Cn. Even chunks and odd chunks are separated. After it, even chunks will be encrypted using ECC algorithm and odd chunks will be encrypted using BLOWFISH algorithm, then it will generate cipher chunks.

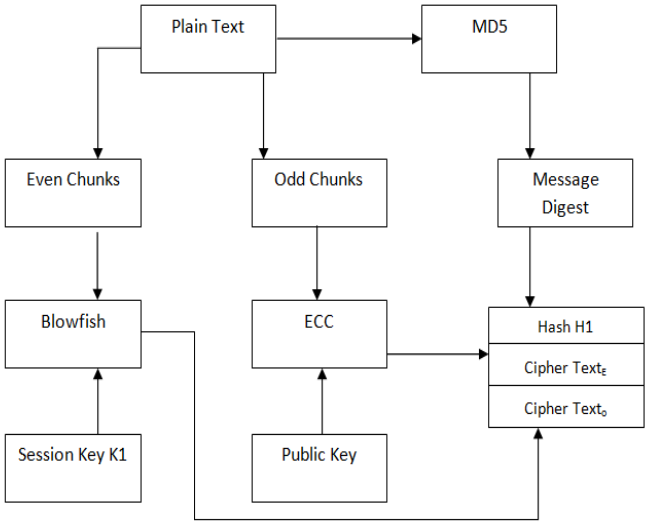


Figure 5. Block diagram of Encryption Architecture.

D. *Decryption Model*

Decryption process, where the ciphered chunks will be taken, then even and odd chunks are identified. Even chunks are decrypted using ECC to get a plain even chunk and odd chunks are decrypted using BLOWFISH to get a plain odd chunk. These chunks are rebuilt to get the complete file.

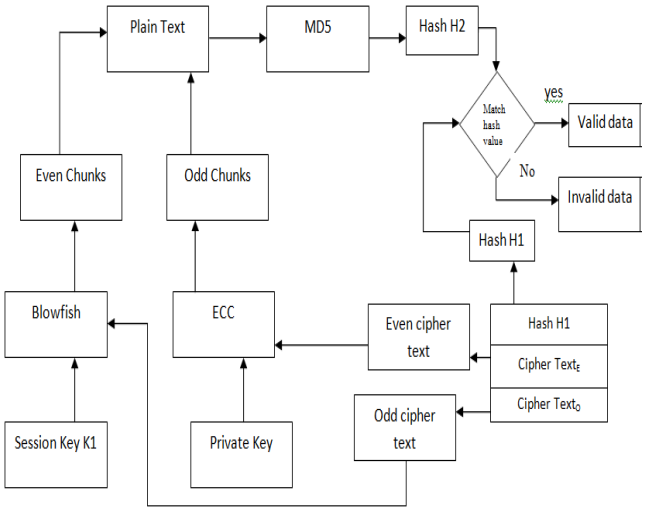


Figure 6. Block diagram of Decryption Architecture

© 2019, IJCSE All Rights Reserved

E. Integrity Comparison Model

Re-calculation of the integrity of the chunk file will be performed using MD5. After it, the re-calculated file Hash 2 will be compared with the calculated file Hash 1, if matched then is accepted and not then rejected.

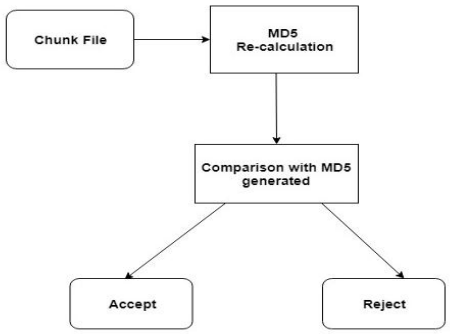


Figure 7. Block diagram of Integrity Check.

IV. RESULTS AND DISCUSSION

The proposed algorithm will provide confidentiality, integrity, and authentication in web applications. It will also reduce the encryption/decryption time to provide a fast way to secure information. To achieve this result we will use Blowfish and ECC algorithm. The intruder will not identify the proposed algorithm because it is more protected. The proposed methodology is executing using Java technology.

V. CONCLUSION AND FUTURE SCOPE

All web applications client always demands security and data privacy to keep their data safe and secure. An enhancement is expected in the security model of existing solutions to raise the level of safety. In the proposed solution, we try to ensure confidentiality, integrity, and authenticity to secure data in web application. The proposed hybrid algorithm combines characteristics of ECC (asymmetric cryptography) which comes with the ease of distributing the key and BLOWFISH (symmetric cryptography) which is easier to calculate and faster, to provide confidentiality. Proposed Technique will provide a good and fast way of securing information in web applications.

We can also use some method to reduce the encrypted data size. Our future work will be on reducing the encrypted data size without compromising with encryption and decryption time. The proposed algorithm can also be implemented for different types of data other than text files. In future, it can be used in particular applications like military applications, hardware and software companies that need security in their products, big websites that have big databases, mobile applications, cloud based applications.

ACKNOWLEDGMENT

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

REFERENCES

[1] K. M. Abdullah, E. H. Houssein, H. H. Zayed, "*New Security Protocol using Hybrid Cryptography Algorithm for WSNs*", 1st International Conference on Computer Applications & Information Security (ICCAIS 2018) IEEE, **Saudi Arabia**, **2018**.

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

[3] M. Harini, K. Pushpa Gowri, C. Pavithra, M. Pradhiba Selvarani, "*A Novel Security Mechanism using Hybrid Cryptography Algorithms*". International Conference on Electrical, Instrumentation, and Communication Engineering (ICEICE) IEEE, **India**, **2017**.

[4] Jayraj Gondaliya, Jinisha Savani, Vivek Sheetal Dhaduvai, Gahangir Hossain, "*Hybrid Security RSA Algorithm in Application of Web Service*". 1st International Conference on Data Intelligence and Security (ICDIS) IEEE, **USA**, **2018**.

[5] Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, "*Hybrid RSA-AES Encryption for Web Services*". International Journal of Technical Research and Applications, Issue. **31**, pp. **51-56**, **2015**

[6] Kirtiraj Bhatele, Prof Amit Sinhal, Prof Mayank Pathak, "*A Novel Approach to the Design of a New Hybrid Security Protocol Architecture*". International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) IEEE, **India**, **2012**.

[7] S. Dubey, R. Jhaggar, R. Verma, D. Gaur, "*Encryption and Decryption of Data by Genetic Algorithm*", International Journal of Scientific Research in Computer Science and Engineering, Vol. **5**, Issue. **3**, pp.**42-46**, **2017**.

[8] M. Amjad, "*Security Enhancement of IPV6 using Advance Encryption Standard and Deffie Hellman*", International Journal of Scientific Research in Network Security and Communication, Vol. **5**, Issue. **3**, **2017**.

[9] B. Hari Krishna, Dr. S. Kiran, G. Murali, R. Pradeep Kumar Reddy, "*Security issues in Service Model of Cloud Computing Environment*", International Conference on Computational Science, Procedia Computer Science 87, **India**, pp.**246-251**, **2016**.

[10] K. Ruth Ramya, T. Sasidhar, D. Naga Malleswari & M.T.V.S. Rahul, "*A review on Security aspects of Data Storage in Cloud Computing*", International Journal of Applied Engineering Research, Vol **10**, No. **5**, pp.**13383-13394**, **2015**.

[11] Rizk, Rawya, and Yasmin Alkady, "*Two-phase hybrid cryptography algorithm for wireless sensor networks*", Journal of Electrical Systems and Information Technology, Vol. **2**, Issue. **3**, pp.**296-313**, **2015**.

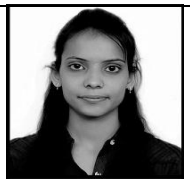
[12] Trishna Panse, Vivek Kapoor, Prashant Panse, "*A review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission*", International Journal of Information and Communication Technology Research, Vol. **2**, No. **3**, **2012**.

[13] Dr. V Kapoor, R Yadav, "*A Hybrid Cryptography Technique to support Cyber Security Infrastructure*", International Journal of Advanced Research in Computer Engineering & Technology, Vol. **4**, Issue.**11**, **2015**

© 2019, IJCSE All Rights Reserved

[14] V Kapoor, R Yadav, "*A Hybrid Cryptography Technique for improving Network Security*.", International Journal of Computer Applications, Vol. **141,** No.**11**, pp.**25-30**, **2016**

Authors Profile



Miss Neha Gupta completed B.E. in Information Technology from Shri Vaishnav Institute of Engineering and Technology, Indore, M.P., India in 2014. She is pursuing M.E. in Information Technology at the Institute of Engineering & Technology, Devi Ahilya Vishwavidyalaya, Indore, M.P., India. Her area of research in Cryptography.

A review on Security aspects of Data Storage in Cloud Computing Mr. Vivek Kapoor is currently working as an Assistant Professor in the Department of Information Technology, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya, Indore, M.P., India. His research interests are Genetic Algorithms, Soft Computing Skills, Information Security.

A review on Security aspects of Data Storage in Cloud Computing Mrs. Jyoti Haweliya is currently working as an Assistant Professor in the Department of Computer Engineering, Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya, Indore, M.P., India. Her research interests are Computer Networks and Compiler Design.

© 2019, IJCSE All Rights Reserved