International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Using A Dual-Layered Security Approach, Cloud-Based Applications Can Be Highly Confidential In The Face of A Crypto Analysis Attack : Review

Dikshika Maliwad Assistant Professor, CSD, Lnct (bhopal) indore campus, Indore

ABSTRACT

Security is one of the important non-functional requirements of every solution. Early days, security and data privacy was just luxury part of software development and it was optional requirement but nowadays, it plays critical role in daily life. This research paper has been made to observe the need of security algorithms in cloud computing. This works observe that 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 RC6 and Blowfish algorithm can be used to achieve confidentiality during communication. The complete work will proposed a security architecture having solution to achieve confidentiality, integrity with strong authentication policy for cloud computing.

INTRODUCTION

Electronic applications keep running on a web application server and access information on a venture data framework, for example, a DB2 database server. The segments of electronic applications are spread over numerous levels, or layers. This data depicts the different segments and building qualities of web applications and the job that DB2 plays in the web application condition. As a rule, the UI is on the primary level, the application projects are on the center level, and the information sources that are accessible to the application projects are on the undertaking data framework level. Creating online applications over a multi-level design is alluded to as server-side programming. 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.

Challenges faced in Web-based Application

1.2.1 User Interface: User interface makes a big impact On a small element. It makes things easy to user, to communicate and use the trending technology. Websites developing requires being responsive for every screen size, which becomes easy to access by the user. If any application creates difficulty forthe user to use, which means the designed user interface is not so good or reliable.

1.2.2 Scalability: Scalability is the balancing of load and managing traffic between servers, this management is possible by adding more servers. Scalability should be achieved by designing software that can work on the cluster of servers.

1.2.3. Performance: Certainly, speed is an important aspect, which shows the performance of any website. Every single second is counted when the business is online. Slow performance leads to failure of application, resulting in escaping websites by customer, negative reputation. Therefore, before developing any application, its performance should be kept in mind. Performance issue comes when the code is not properly written, is not optimized, is not properly managed, poor load balancing, etc. are some of the factors and troubleshooting required for third party services.

1.2.4. Security: With designing for user interface and experience, security is over and over ignored. However, security is to examine throughout the software development life cycle. Application mainly deals with vital information like users' personal information, which is confidential. When dealing with the web application, the safety of user data, service attacks, and unauthorized access is important to measure.

1.2.5. Knowledge of Framework: For knowledge boosting, frameworks are significant to develop languages. It extends capabilities to work and develop a web application from the initial level. The framework offers many features like APIs, code snippets and dynamic elements of the web application. Frameworks have rigid and flexible development approach. PHP, ASP .Net, J2EE, etc. are some of the web frameworks.

1.3 Web Application Security The process of safeguarding sensitive and confidential data which is stored online from modification and unauthorized access is Web application security. This is proficient by implementing strict policy measures. Security threat is that the hackers or intruders with nasty intentions try to access the sensitive information stored by an organization. The main aim of security in a web application is to recognize the following: Critical assets of an organization.

- Authorized users who have rights to access the data of organization.
- The level of rights to access data provided to each user.
- Various weaknesses that may exist in the web application.
- Data criticality and risk analysis of data exposure.
- Appropriate remediation measures.

1.4 Need of Security in Web Application

As the growth of the internet rises the attacks on Web applications are also increases, security must be the prioritize concern to improve the effectiveness of web applications. Earlier, the violation of data was very rare and the data is violated due to the mistake of humans, for example breaking of physical devices like laptop, pen drive, floppy disk. Some other means of data theft is by using the vulnerabilities of web applications, by clicking the wrong link unknowingly. The companies that suffer from data violation or theft may not know the reason behind this or did not put efforts to find it. In recent years, data violation, data theft, and modification by intruders increase day by day. This unauthorized access of sensitive data of people, organization forces the government to start the laws for data privacy like GDPR. To provide the security to the Web application is very important because web applications are exposed to the internet and most of the unauthorized access and modification of data is done through it. One of the studies shows that 77 percent of web applications have at least one security weakness. For attackers to successfully installed the malware, to remotely control the exposed computer without coming in the notice and to find the data to steal required a large time which increases the chances of being caught. As a result, attackers try to access sensitive data by using the vulnerabilities of web application security. These types of attacks are more efficient and effective. The web application vulnerabilities give some way to attackers to freely access the data that is stored on that server. The organization will have to use the high level of security to protect their websites and applications sensitive and critical data from attackers because to exploit the web application security attackers use security vulnerabilities to access the critical or sensitive data. The capacity to safely store and move sensitive data has demonstrated a basic factor in progress. It is essential to verify Data for a private transmission. It winds up basic to shield data from unapproved clients. This data ought to be accessible, open just for the approved clients, and ensured by unveiling and making it inaccessible for unapproved clients. Subsequently, privacy respectability and accessibility turn into the most significant elements for secure information transmission.

LITERATURE REVIEW

The literature survey describes the work is done by others. Algorithm and techniques used in already implemented or proposedwork done by othersand the mitigation approach discovered, explaining the methods evolved for the improvement of basic versions.

Khalid M. Abdullah et al. In[1] proposed hybrid security protocol, consolidates attributes of the asymmetric key cryptography which provide an easy wayto share the key and symmetric cryptography which is simpler to compute and quicker. In the proposed work RSA and AES are used for encryption-decryption and LZW compression technique is used to compress the size of cipher text. They divide the data into chunks, generate the AES key to encrypt the odd chunks and to encrypt the even chunks RSA algorithm is used. To send the AES key, it is further encrypted using the RSAprivate key. After encryption compresses the cipher text using LZW

Jayraj Gondaliya et al. In [2] proposed another crossbreed security cryptosystem, Hybrid RSA, by utilizing results over two huge prime numbers in the RSA-based cryptosystems to expand the multifaceted nature of splitting the framework. The proposed Hybrid security calculation for RSA called HRSA was demonstrated proficient. The key generation time, encryption time and decoding time are the principal parameters estimated for productivity. The problem with this model is that it can not be used for low powered device. If large prime numbers are used then it will take more time to generate the key, encrypt/decrypt the data

V. Kapoor, Rahul Yadav In [3] proposed a cryptographic technique for improving network security. They find a strong encryption algorithm that can be proficiently works on the different kinds of data and produces the multifarious cipher text. Therefore, a hybrid cryptographic algorithm is prepared using RSA, DES and, SHA1. To enhance the encryption process and the secure key generation they implemented a bit discarding process. This process reduces the key size and improving the complexity of the key generation process. In the proposed algorithm the hash code of plain text is calculated using SHA1, using the hash code generate a key which is used to encrypt the input file using the RSA algorithm. Then the DES algorithm is used to further encrypt the key used in encryption to make it secure. To implement the proposed hybrid encryption technique, they useJAVA technology. Additionally, check the estimated performance of their algorithm in terms of encryption time, decryption time and space complexity. Also, compare the obtained performance of the proposed cryptographic solution with the traditional RSAalgorithm for a similar size of the file.

F. F. Moghaddam et al. In [4] proposed an authentication scheme for the cloud environment. This paper addresses the issues of scalability, trust, and efficiency in user authentication for the cloud environment. One of the schemes is client-based authentication, which is used toauthenticate the registered user at the client side. AES-192 algorithm is used to provide encryption. To access the cloud servers for the un-registered user a modified Diffie Hellman algorithm is used to provide authentication on the cloud. To reduce the dependency of authentication and encryption from the main server they use two separate servers. In this paper,the theoretical analysesstates that the scheme provided by them are reliable and increase the rate of trust in the cloud environment.

Kirtiraj Bhatele, A. Sinhal and Mayank Pathak [5] introduces a new security protocol for Online transactions using the symmetric key and asymmetric key cryptography. The paper is taken into consideration that in online transactions security should be high with less communication time. The hybrid model uses ECC, AES, RSA, MD5 and, Dual RSA to achieve three principles of security that is integrity, confidentiality and authentication. The proposed algorithm helps in providing low power consumptions, the efficiency of storage and saving the bandwidth for applications where these parameters are highly recommended. This work uses AES to encrypt the data, MD5 to maintain the integrity and Dual RSA to encrypt the hash value calculated by MD5 to make it hard for intruders to decrypt it.

Yasmin Alkadey et al. In[6] proposed hybrid protocol AES, ECC, Dual RSA with XOR and MD5 is used to provide security in WSN. In this research work they compare proposed hybrid protocol with existing algorithms in terms of power consumption, rate of dropped packets, size of the encoded file, time consumed in encryption/ decryption and throughput. XOR-Dual RSA is used to provide authentication, MD5 for the integrity of the message and AES combined with ECC to encrypt the node.

Vivek Kapoor et al. In [7] proposed a cryptography algorithm to Improve Data Security. Proposed Cryptographic Algorithm is used to achieve confidentiality, whereas Message Digest Algorithm MD5 is used to maintain the originality of the message.RSA is used to solve the key distribution problem to strengthen the security of transmitted data and to generate the digital signature.

Amrita Jain and V. Kapoor In [8] proposed work analyzed the existing problem inthe network environment.In the network environment, secure communication is the basic requirement to utilizefar-off resources in an efficient and controlled way. The Monitoring tool required complex processing due to the very large size of information generated by it. In this paperto take the timely response and to improve the security situation detection an ICARFAD based assessment mechanism is proposed. It has fourphases an information collection, assessment, response and, feedback. This work uses various parameters to calculate the accurateperformance of the system. This work provides effective results in the future.

PROBLEM DEFINITION

The Problem of the complete project defines the need of security parameter where security is essential to preserve any sensitive data. Sensitive data can be personal data or information related to details which should not be known to anyone. Another issue is the trust issue where the third party vendor outsources their data for user’s use. User does not trust on third party or sometimes it happens that the third party vendors are not trustworthy. Authentication and authorization are the major security concern, which needs to be resolved so that only the authorized person is valid to perform login and access operation. User, which performs an unauthorized activity, is the malicious attacker or intruders that need to be preserved and diagnosed at the right time for future security purpose.

METHODOLOGY

The proposed methodology describes a secure encryption/decryption process by generating the key, where the base key is used in generating the number of keys K1, K2,..,Kn. After Key Generation process, it performs authentication to authenticate the client who wants to access the resources of web application using a modified Kerberos protocol. Once the authentication server authenticates the client the resource server gives access to its resources.On the data uploaded by the client to achieve confidentiality, weperform encryption/decryption using ECC and RC6 algorithm. It also uses MD5 algorithm to preserve the integrity of data. The Flow ofthe complete architecture is shown below: Plain text is taken.

- Plain text is divided into chunks
- Chunk C1, C2, C3 and C4.
- Odd and even chunks are separated.
- Odd chunks are encrypted using RC6 algorithm, and
- Even chunks are encrypted using ECC algorithm.
- The Plain text then encrypted and converted into cipher text.

OBJECTIVE

The Objective of the complete work is as follows:

- To implement confidentiality using ECC and RC6 algorithm.
- To diagnose and mitigate the issues evolved in existing work.

- Divide data into chunks to make the encryption process as fast as possible.
- To achieve integrity using MD5 algorithm.
- To Achieve authentication using modified Kerberos.

PROPOSED SOLUTION

Web applications aid the system with cross-platform functionality regardless of the software and messaging 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 aspossible. In the proposed hybrid algorithm we replaced the AES algorithm by RC6 security algorithm, which is faster than AES and ECC algorithm with RSA algorithm. ECC algorithm can provide the same level of security afforded by RSA with a large modulus and corresponding large key. To verify the originality of data we implemented MD5 algorithm and to authenticate the client we apply modified Kerberos protocol.

CONCLUSION

The rise in Internet use and automation of regular industry will influence the way of business. Nowadays,to showcase a business or to compete with the others in the competitive world people are migrating their business to the web platform instead of only shop-based approach.Web applications provide businesses the ability toreduce costs, intensify efficiency, and modernize their operations. All the clients who use web applications always demand security and data privacy to keep their information safe and secure from unauthorized access. In the security model of existing solutions an enhancement is expected to raise the level ofsecurity. In the proposed hybrid model, to safe guard the data from unauthorized access in web applicationwe try to ensure authentication, confidentiality, and integrity. In the proposed hybrid model,to achieve confidentiality we combine the good features of both asymmetric key cryptography (ECC) which comes with the advantage of distributing the key and symmetric key cryptography (RC6) which is faster and easier to calculate. Proposed Hybrid Model provides the best and fast way of safeguarding the data in web applications.

FUTURE DIRECTIONS

During Implementation, we observe that the encrypted data size is large that the plain text. In the future, the encrypted data size can be reduced without negotiating with encryption and decryption time. The proposed hybrid model can also be implemented for different files types other than .txt files for example .mp4, .doc, etc. In the future, it can be used forspecific 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..

REFERENCES

[1].Khalid M. Abdullah Essam H. Houssein Hala H. Zayed, “New Security Protocol using Hybrid Cryptography Algorithm for WSN”. 1st International Conference on Computer Applications and Information Security (ICCAIS), IEEE, 4-6 April. 2018

[2].Milind Mathur, Ayush Kesarwani, “Comparison between DES, 3DES, RC2, RC6, RC6, andAES”. Proceedings of National Conference on New Horizons in IT – NCNHIT 2013.

[3].V. Kapoor, Rahul Yadav, “A Hybrid Cryptography Technique for Improving Network Security”, International Journal of Computer Applications, Volume 141, No.11, May 2016.

[4].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 2017.

[5].Kalyani Ganesh Kadam, Prof. Vaishali Khairnar, “HYBRID RSA-AES ENCRYPTION FOR WEB SERVICES”. International Journal of Technical Research and Applications, Issue 31(September 2015), PP. 51-56.

[6].F. Fatemi Moghaddam, S. Gerayeli Moghaddam, S. Rouzbeh, S. Kohpayeh Araghi, N. Morad Alibeigi, and S. Dabbaghi Varnosfaderani, “A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments,” in IEEE Region 10 Symposium, Kuala Lumpur, Malaysia, 2014, pp. 508–513.

[7].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 IEEE 2018.

[8].KirtirajBhatele, ProfAmit Sinhal, ProfMayank 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 2012.

[9].A. Arjuna Rao, K Sujatha, A Bhavana Deepthi, L V Rajesh, “Survey paper comparing ECC with RSA, AES and RC6 Algorithms”. International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 1, IJRITCC January 2017.

[10]. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk, “A New Security Protocol Using Hybrid Cryptography Algorithms”. 9th International Computer Engineering Conference (ICENCO), IEEE 2013