ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 8(S2), 160–164, January 2015*
DOI: 10.17485/ijst/2015/v8iS2/60449

Secured Transaction for Distributed Service System

M. Abhinivesh, Mayank Garg, Karishma and D. P. Acharjya

School of Computing Science and Engineering, VIT University, Vellore-632014, Tamilnadu, India; dpacharjya@gmail.com

Abstract

With the rapid growth of networking and Internet-dependent activities in our daily lives, security has become an important issue. In general, security is more important when concerned to web services and on-line transactions. Web services in general has configuration that represents the constraints and capabilities of the security policies at both internal and end node. It defines security index that are acquired, encryption algorithms that are used, and privacy rules that has to be employed at all nodes. Present realizations of Advanced Encryption Standard (AES) on Reduced Instruction Set Computing (RISC) do not support encryption and decryption. In addition, it only allows a specific cipher block size. In order to overcome the limitations, in this paper we propose and analyze a secured system web service which generate dynamic key and support parallel encryption and decryption.

Keywords: Data security, Decryption, Distributed System, Encryption, System Security, Web Services

1. Introduction

The convergence of information and communication technologies drastically changed our daily lives. It is achieved with the help of vast growth of internetworking and Internet-dependent activities. On the other end, it leads to security issues for a common man. The security concerns are manifold: If the computer in the network is viewed as a trustworthy box containing only legitimate software, then security concerns relate to data in transit. The main concern here is that all communications take place over public networks and these networks accessible to anyone. Therefore, it is essential to prevent the sensitive data from stealing. This leads to data security. Another concern is the trustworthiness of the machines that a common man works with. Data thieves constantly attack the computing equipment by sending virus and worms. It leads to system security. Therefore, security is a major and challenging issue in current research.

Present information technology service system is relying upon collection of different services protocols security encryption. The operating efficiency, quality of services and work flow of these protocols is categorized into different privacy regulations[6]. Encryption service is important because it is needed for transmission of information and authentication for verify excess level of user. On the other hand, distributed systems are helpful in gathering and processing information about users of a particular domain by means of efficient communication techniques between models for an effective sharing of resources. It access web services and web portal authentication in the form of identities. The authentication rules can be defined by a programmer. In addition, it utilizes the web services information with security. To approach this issue through web services packet classification for network intrusion detection using Field Programmable Gate Array (FPGA) is introduced[15]. But, for different level of user access, some restriction and security is needed. In order to improve this information technology services one has to follow web services standard[7,8] and security algorithm like AES[1–4]. For creating and deploying the web services we need network protocol and web service architecture. In general, the implementation of the secured information technology system web services requires Intrusion Detection Systems (IDS)[9,10] and Intrusion Prevention System (IPS). It prevents to upload any malware and software which has security breach like Trojan[6]. Keeping view to all these, the development of web services and computer network include instruction prevention system[12] and instruction detection system. In addition, firewall and network

*Author for correspondence

devices are used to prevent the attack from the intruder by database hacking[13]. Generally intrusion detection system is used for monitoring the root, location and then informs the administrator if network behavior is abnormal.

The proposed model can identify the malicious software or program by detecting disturbances in the network behavior. The proposed model uses dynamic key generation for various information sets in advanced encryption standard algorithm and hence is not complex. In addition, the deploying cost is very less. The rest of the article is organized as follows: Section 2 provides related works in the direction of secured transaction for distributed service system. We propose the model in Section 3 followed by results, discussion and implementation in Section 4. Finally, the article is concluded in Section 5 with conclusion and future extension that can be made to the proposed system.

2. Related Work

Web service has transactions of information in the form of web applications, web portal and web site. Security for these services acquires encryption techniques. This is achieved in many ways. Performance of AES candidate algorithms in java[3] suggests that it has some space for enhancement by dynamic key generation. Fast implementation of AES candidates[1] suggests how encryption process can be speed up and enhance the security. However, it has certain limitations. Some limitations include time constant, and data reliability. The secure and efficient AES software implementation for smart cards[4] uses AES encryption algorithm with symmetric key approach. It has applied on 128, 192 and 256 bits size of key because of variability data masking technique. The main limitation of that experiment is extra time consumption in process block which is used for exclusive OR (XOR) masking. It has iterative process based on block size program that iterates for both encryption and decryption.

It is well understood that, these researches use AES encryption algorithm but they did not consider time. Keeping view to this, in this paper we consider time as a constraint and deployed our security service in web service based application. Existing web services approaches follows standard and services such as service transport, XML messaging[11], service description and discovery. The web service architecture includes the web service role and web service protocol stack. The web service role consists of service provider, service requestor, and service registry. Service provider implements the services and put it into Internet for making service availability. Service requestor requests the existing services in the form of XML request[5]. Service registry is used to centralize directory of services. It provides a place where to deploy their web service or find existing one. All these implementation of the secured service system of web services involves IDS and IPS[14]. Saffa Zaman and Fakhri Karray proposed lightweight intrusion detection system based on features selection and classification[9] to attain web service security. On the other end, S. Roschke et al uses an extensible and virtualized compatible intrusion detection system management architecture for attaining web service security[10]. G. Chen et al. discuss wireless intrusion prevention systems based on plan recognition and Honeypot[12]. In addition, all these follow web services standard[7,8]. In the following section, we present brief foundation of web service protocol stack.

2.1 Foundations of Protocol Stack

In this section for better understanding, we provide brief description and terminologies of protocol stack that is used in web services[15–17]. It includes service transport, description and discovery, extensible markup language (XML) messaging, web services description language, input and output message format and port which are as follows:

Service transport layer is used for sending messages from one application to another application whereas service description is used for explaining the interface to a particular web service. Service discovery is used for explaining the interface to a specific web service. XML Messaging is used for encoding simple messages into a general XML format in order to understand the messages that can be presented at either end. Web services description language (WSDL) is used for describing a web service which is present in XML file. Port is used to access the uniform resource locator (URL) of the web service. Universal description, discovery and integration (UDDI) is used to register WSDL and make the web services is visible through the internet for discovery. Web service reliable messaging uses the protocol that includes simple object access protocol (SOAP). It is because; secure transfer of messages between different distributed web applications. Web service security is an enhancement to SOAP messaging security that is available in SOAP message protocol. In general it explains three aspects such as integrity of a SOAP message, confidentiality of the messages and ascertains the sender's identity by attaching security tokens.

3. Proposed Model

Web services describe the policy, transactions and security of components. Security contains encryption algorithms and security tokens. Web service privacy gives the preference to the different level of access in order to organize privacy policy. Web services security is based on different web service protocols like simple object access protocol that provides XML based messaging services. It provides data confidentiality, message integrity and manages certain user identity. In addition, it describes encryption and decryption for maintaining security.

Data exchange is very common while communication between network protocols. It is well understood that, they must follow TCP/IP protocol to send and receive the data. The packet in general contains the confidential information which is to be processed. The packet length should be equal to that of defined in TCP/IP protocol. Deviation to this can not confirm to this is protocol. The process control flow of the proposed model is given in the following Figure 1.

In the process of encryption, the whole packet would be encrypted. In addition, keywords search is the key element in this process. For this magic numbers are used at the beginning of binary data file. Even file extension would also be changed by magic number identification. The keywords search contains a magic number that has confidential keyword which may appear in the packet. Improved sequential search algorithms are generally used to process packet header and also it checks cycle redundancy segment. Network protocol and keyword search matching technique applied to the packets. This helps us differentiate the characteristics of the packets. If any intruder tempers or hack the program, then the packets contain error messages and so cannot be considered as normal packets. It can be easily find that there is temptress in the packet. Data stream control technique is very useful to this end but it suffers from static check method. If the checking is changed to dynamic, then the performance of that program will be increased.

In the existing system the AES algorithm is used but there is no simultaneously encryption and decryption. In addition, the key size is fixed in the existing system. In order to overcome the limitations, in our proposed model data is encrypted and decrypted at the same time. Also, in proposed system, key size is not fixed and changes dynamically. It indicates that, there is dynamic change of bits of encryption key during process. The different length and combinations include bits like 128 bits, 192 bits, 224 bits, 240 bits and 256 bits.

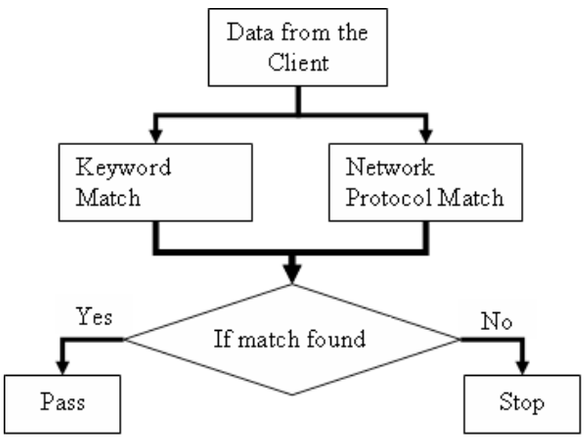

Figure 1. Process control flow of proposed model.

4. Results and Discussions

The proposed model of web service has three modules such as control module, key module and encryption module. Control module contains the basic web service for distributed service system. It includes web services server, web service client and SOAP protocol. After defining this basic web services, the key module has included. Key module contains size of a key for the encryption purpose. The keys are dynamically generated based on the size of data. Simultaneously, it enhances the time complexity of the algorithm. The encryption module contains AES encryption algorithm that provides encryption and decryption for data security. Implementation of AES algorithm is carried out using Java language. The following Figure 2 provides the effective implementation of proposed model.

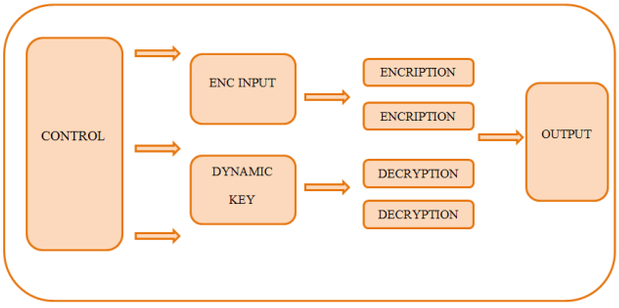

Figure 2. Basic architecture of AES module.

In general, key size is responsible for secure transactions in a distributed service system. Figure 3 depicts how key size changes dynamically with the data size. In Figure 4, it has shown that based on key size how the execution time fluctuates. It is because; if key is complex it will take more time for decryption as well as more time to make such complex keys. Figure 5 depicts how different data size has different execution time. It is also observed that, if the data size increases then the execution time for encryption as well as for decryption also increases.

In Figure 6, it has shown that at some point, the execution time remains constant. It is because of dynamic key size that provides particular data size is ambient to particular key size. Therefore, it provides optimum result for time constraint. Figure 7 describes that speed up in different cores when number of processers increases the speedup is almost constant because of parallel overhead.

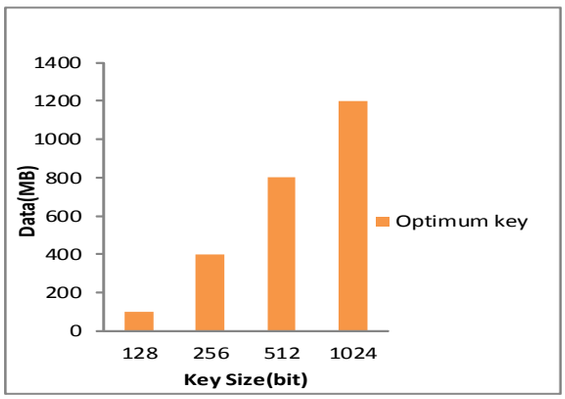

Figure 3. Optimum key size for different data size.

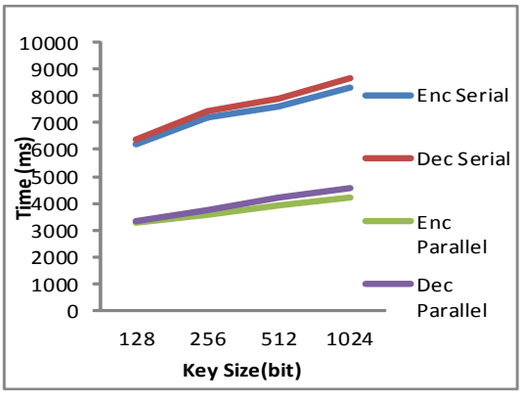

Figure 4. Execution time depending on key size.

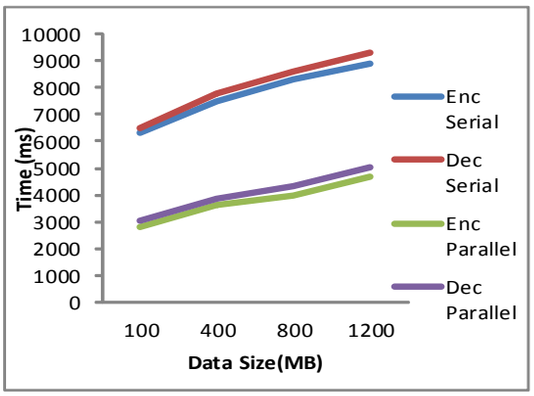

Figure 5. Execution time for different data sets.

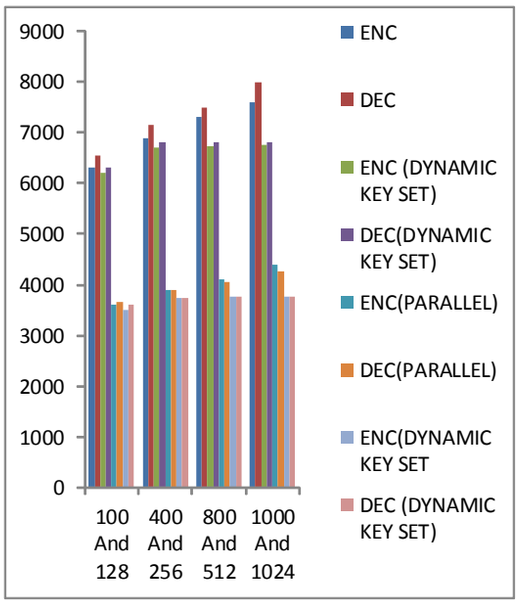

Figure 6. Execution time for different data size and key size.

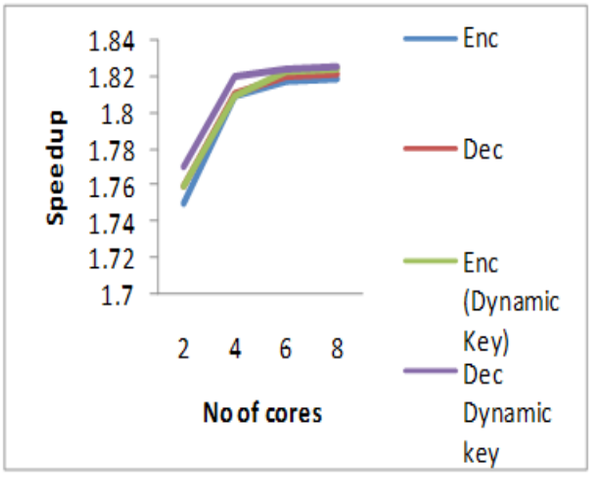

Figure 7. Speed-up comparison in different cores.

5. Conclusion

This paper extends the AES algorithm to advanced AES coding formula in web services to produce secured transition in distributed system. In this model, the dynamic key generation for various information sets is applied. In addition, parallel coding is co-jointly enforced. Services like SOAP and REST is used to implement security. Dynamic key provides higher leads in terms of time constraint by providing optimum key size for information sets. It is observed that, the technique is powerful and secured for web services. Also, it can be enforced in any distributed service system. The module is tested in numerous personal networks and found satisfactory. Future prospective of this research work can be carried out in the direction of raising potency of AES realization for information processing and spoofing.

6. References

1. Aoki K, Lipmaa H. Fast implementations of AES candidates. Proceedings of 3rd Advanced Encryption Standard Candidate Conference. New York; 2000 Apr 13-14. p. 106–22.
2. Trichina E, Korkishko L. Secure and efficient AES software implementation for smart card. Berlin: Springer Berlin Heidelberg; 2005.
3. Sterbenz A, Lipp P. Performance of the AES candidate algorithms in java. Proceedings of 3rd Advanced Encryption Standard Candidate Conference; 2000 Apr 13-14; New York. p. 161–8.
4. Schramm K, Paar C. IT security project: implementation of the Advanced Encryption Standard (AES) on a smart card. Proceedings of the International Conference on Information Technology: Coding and Computing; 2004 Apr 5-7; Germany. p. 176–80.
5. Peter F, Schneider P, Simeon JO. Building the semantic web on XML. The First International Semantic Web Conference; 2002 Jun; Italy. p. 582–7.
6. Zhang X, Li C, Zheng W. Intrusion prevention system design. Fourth International Conference on Computer and Information Technology; 2004 Sept 14-16; China. p. 386–90.
7. Squicciarini AC, Carminati B, Karumanchi S. Privacy aware service selection of composite web services invited paper. 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing; 2013 Oct 20-23; USA. p. 260–8.
8. Bui NB, Zhu L, Liu YJ, Tosic V, Jeffery R. Automating web service development using a unified model. 12th Enterprise Distributed Object Computing Conference Workshop; 2008 Sept 16; Sydney. p. 301–8.
9. Zaman S, Karray F. Lightweight IDS based on features selection and IDS classification scheme. International Conference on Computational Science and Engineering; 2009 Aug 29-31; Canada. p. 365–70.
10. Roschke S, Cheng F, Meinel C. An extensible and virtualization-compatible IDS management architecture. Fifth International Conference on Information Assurance and Security; 2009 Aug 18-20; Germany. p. 130–4.
11. Specification for the Advanced Encryption Standard (AES): Federal Information Processing Standards Publication 197; 2001.
12. Chen G, Yao H, Wang Z. Research of wireless intrusion prevention systems based on plan recognition and honeypot. International Conference on Wireless Communication and Signal Processing; 2009 Nov 13-15; Nanjing. p. 1–5.
13. Sharlin N, Judith, Bairavel S. Preventive approach to avoid intrusion in relational databases using response patterns. Third International Conference on Sustainable Energy and Intelligent System; 2012 Dec 27-29; India. p. 1–6.
14. Stanton R, Head G. Securing VPNs: comparing SSL and IPsec. Fifth International Conference on Information Assurance and Security; 2005 Aug 18-20; Germany. p. 17–9.
15. Song H, Lockwood JW. Efficient packet classification for network intrusion detection using FPGA. Proceedings of the 2005 ACM/SIGDA 13th International Symposium on Field-programmable gate arrays; 2005 Feb 20-22; Monteney. p. 1–7.
16. Durmus A, Erdogan N. A web services market framework with role based agents. IEEE International Conference on Systems, Man and Cybernetics; 2009 Oct 11-14; Turkey. p. 4722–7.
17. Bajpai V, Schonwalder J. Measuring TCP connection establishment times of dual-stacked web services. 9th CNSM and Workshops; 2013 Oct 14-18; Germany. p. 130–3.