International Journal of Information Technology and Management

A NEW MODEL METHOD TO SECURE AN E-COMMERCE WEBSITE

Nimish Shah, Laksh Gupta, Mihir Srivastava and Shourya Maheshwari,
School of Computer Science and Technology,
Vellore Institute of Technology,
Vellore, India
Email: nimishtarang.shah2018@vitstudent.ac.in, laksh.gupta2018@vitstudent.ac.in, mihir.srivastava2018@vitstudent.ac.in, shourya.maheshwari2018@vitstudent.ac.in.

Abstract: We looked into the security design of many websites both e-commerce related and on other websites, we noticed some serious structural deficiencies. So in this paper we have come up with a new approach to securing a website. We plan to utilise the Asymmetric Key Cryptography Algorithms like RSA to overcome the vulnerabilities to some extent. We focus especially on the client server communication aspect of the website, where we use multiple techniques like diffie-hellman key exchange for each user as soon as he signs up. During Sign Up the client and server exchange symmetric keys. This key is then used to encrypt and decrypt all further communication after the login period using the AES algorithm.

Keywords: Asymmetric Encryption, RSA, Public Key, Symmetric Encryption Private Key, AES.

Introduction

Our new security design implemented here for an e-commerce website will be a new and secure way for handling the security of a website. It will prevent attacks and ensure confidentiality, integrity and availability for the website for the users.

Existing methods are often not secure enough and were built incrementally, modified to address any new threats, our model is a complete model built from scratch using the latest algorithms for encryption and hashing like AES, RSA-3072 bit and Blake2b. These algorithms are both faster and more secure than legacy algorithms.
Security Requirements provided in our system security requirements for a website are authorization, authentication, non-repudiation and data protection.

Authentication

Authentication means ensuring that every party involved in using the website—the user, the server, and the ISP —is what it actually claims to be. Authentication involves getting credentials of the website(like its digital signature) and confirming them against a trusted third party.

Authorization

Authorization means the person making the request should be the person they claim to be and there should be some form of access control systems in place to confirm this. Also once identity is confirmed the person would only be allowed to make specific requests based on their

predetermined access level.

Data Protection

Protection of data means that the request made to the website and response json that we get have not been altered or tampered while in transit. It is ensuring both data integrity and privacy.

Nonrepudiation

Nonrepudiation basically means accepting that you are sending the data. Once a data is sent, the sender then cannot deny that they did not send the data, there will be proofs that say the sender is in fact the sender receiver is claiming to be.

Security threats

Existing security architectures can have many structural vulnerabilities. some of these are

A. Man in the middle attack

In these attacks the attacker intercepts the traffic between the client and server and may attempt to tamper the message, delay the message(replay attack), may try to read the message, try to impersonate the sender(IP Spoofing) or simply just hijack the session that was established between the client and the server.

B. Attacks through proxy servers

While not exactly an attack, this is a major setback in multi tier architectures or if the ISP is passed through a proxy. A proxy server acts as a middleman between original communicators. Now the proxy server can easily listen to or leak the communication as it needs to transfer data through it, so attacks on proxy servers is a major threat as data can be easily obtained through them.

C. DOS and DDOS attacks

In these attacks the attacker attempts to overwhelm the server by sending multiple fraudulent and incomplete requests , with so many incoming requests the server is not able to respond to legitimate requests and the system becomes inaccessible.

D. Birthday attack

Birthday attacks are made against hashing algorithms that are used to verify the integrity of a message. A message processed by a hash function produces a message digest. This digest can uniquely characterize the message. The birthday attack refers to the probability of finding two random messages that generate the same digest when processed by a hash function. If an attacker can calculate the same digest for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares digests.

E. Cross Site Scripting Attacks

Cross site scripting attack or XS attack is when the attacker injects some javascript code to the website on client side to make the website execute the code.XSS attacks aim to target the users of a web application, and they may be particularly effective because they appear within a trusted site.

F. SQL Injection

A SQL injection occurs in the website when an attacker tries to insert malicious code into our server and gets to our database and makes changes in the queries.

G.Eavesdropping attack

This attack occurs when someone is intercepting your network . Attackers can obtain passwords, bank details and other confidential information by eavesdropping. Eavesdropping is of two types-

1)Passive eavesdropping- attackers can see the information which is intercepted.

2)Active eavesdropping- attackers can see the information and can also temper the information.

Some modules of this research are:

A. *Diffie hellman Algorithm*

Diffie-Hellman is a very popular technique used to exchange keys over an unsecure public network. the keys are not ever actually exchanged; they are derived individually by both parties at their end.It is named after their inventors Whitfield Diffie and Martin Hellman.

If two parties(Alice and Bob) want to use Diffie-Hellman, they first agree between them a large prime number p, and a generator g (where $0 < g < p$).

Alice chooses a random secret integer a (private key) and calculates g^a mod p (which is her public key and is sent over the unsecured channel). Bob chooses his private key b, and does the same.Now Bob knows b and g^a(sent by Alice to him) , so he then calculates (g^a)^b mod p = g^ab mod p. Alice also knows a and g^b, so she can calculate g^ab mod p. Therefore both Alice and Bob have generated a shared secret g^ab mod p. An attacker can know the value of p, g, g^a mod p and g^b mod p. However the attacker will be unable to calculate the shared secret from these values and alice and bob would have shared a secret symmetric key.

B. *Symmetric key Cryptography*

In Symmetric-key encryption, the message is encrypted and decrypted using a key and with the same key. as opposed to asymmetric key Cryptography where separate keys are required to encrypt and decrypt a message. Usually resource utilization is lower than asymmetric key encryption. but key manage=ment becomes very important. Eg. DES, 3DES, AES, and RC4.

C. *JSON web Token*

JWT tokens are used widely in the IT industry to authorize the logged in user. It is digitally signed and can also be used to exchange information.

JWT Tokens have 3 parts, separated by dots,

1. *header: consists of token type and the signing algorithm used.*
2. *payload: It contains claims, the information that we want to encrypt or exchange.*

3. *signature: Basically a MAC code to ensure the message hasn't changed along the way.*

The tokens can be generated on the server and client can store it in browser and use it as a header value while sending the request on the server and server decodes the token and ensures that user is who he says he is (Authorization property)

D. AES Algorithm-

AES(Advanced Encryption Standard) algorithm is also known as the Rijndael algorithm. It is a block cipher with a length of 128 bits. It allows for three different key lengths 128, 192, 256 bits. AES encryption for 128-bit keys has 10 rounds ,192-bit keys has 12 rounds, 256-bit keys has 14 rounds.

Steps performed in each round-

1)Substitution of the bytes

2)Shifting the rows

3)Mixing the columns

4)Adding the round key

Encryption Process-

Performing the encryption process of the given plain text block using four different transformations in the initial round, the 9 main rounds and the final round.

SubBytes

First do xor of initial input and cipher key in 1st round, for remaining 9 rounds we will substitute values with help of substitution box.

Shiftrows

In this step we shift rows, we are given four rows and four columns. First row remains the same, the second row is rotated by one byte, the third row is rotated by two byte, and the fourth row is rotated by three byte.

MixColumns

The Hill cipher is used to jumble up the message more by mixing the block's columns.

Addroundkey

We will take a xor of message and respective round key.

Decryption Process

The pattern of disentangling of an AES ciphertext resembles the encryption connection in the opposite demand. Each round contains the four cycles drove in the contrary solicitation −

1)Add round key

2)Mix columns

3)Shift rows

4)SubBytes

Since sub-measures in each round are in reverse, not in the least like for a Feistel Cipher, the encryption and unscrambling estimations ought to be freely done, notwithstanding the way that they are solidly related.

AES Analysis

AES is widely supported in both hardware and software. Till date, no feasible cryptanalytic attacks against AES have been found. Besides, AES has intrinsic flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform complete key requests. Regardless, also as for DES, the AES security is ensured simply if it is successfully completed and extraordinary key organization is used.

2. Background and Related work

The majority of similar analysis stems from two areas: service collaboration prediction methods and proposing specific data/items based on user data.
The other question is how to provide a centralised acquisition service/architecture. Data from users is aggregated, maintained, and used across various services/devices. The recipient is the developer of this software development case.
Programming arrangement is a significant concern during the item improvement process.Design issues are customary stresses among experiences shared by developers.This is fundamental in light of the fact that early arrangement decisions by originators may affect some basic qualities of a system, similar to common sense, energy, understandability, and execution.
While a part of these essential issues of interest are quality concerns (eg, execution, security, steadfastness, usability, etc) which all item should address, various issues oversee crosscutting worries, for instance, the best strategy to fall apart, figure out, and group programming parts.

According to Sousa, an item plan issue happens when an item plan decision has an antagonistic result on in any event one quality attribute of the item. An arrangement issue impacts on a segment of the key properties, (for instance, extensibility and common sense, energy, understandability, and execution) of an item structure. They thought that it is difficult to

perceive an arrangement issue in a structure, and explicitly when the source code is the simply open collectible, it is more hard to recognize the arrangement issues. They deduced that engineers/programming makers oftentimes use different markers during the ID of each arrangement issue.

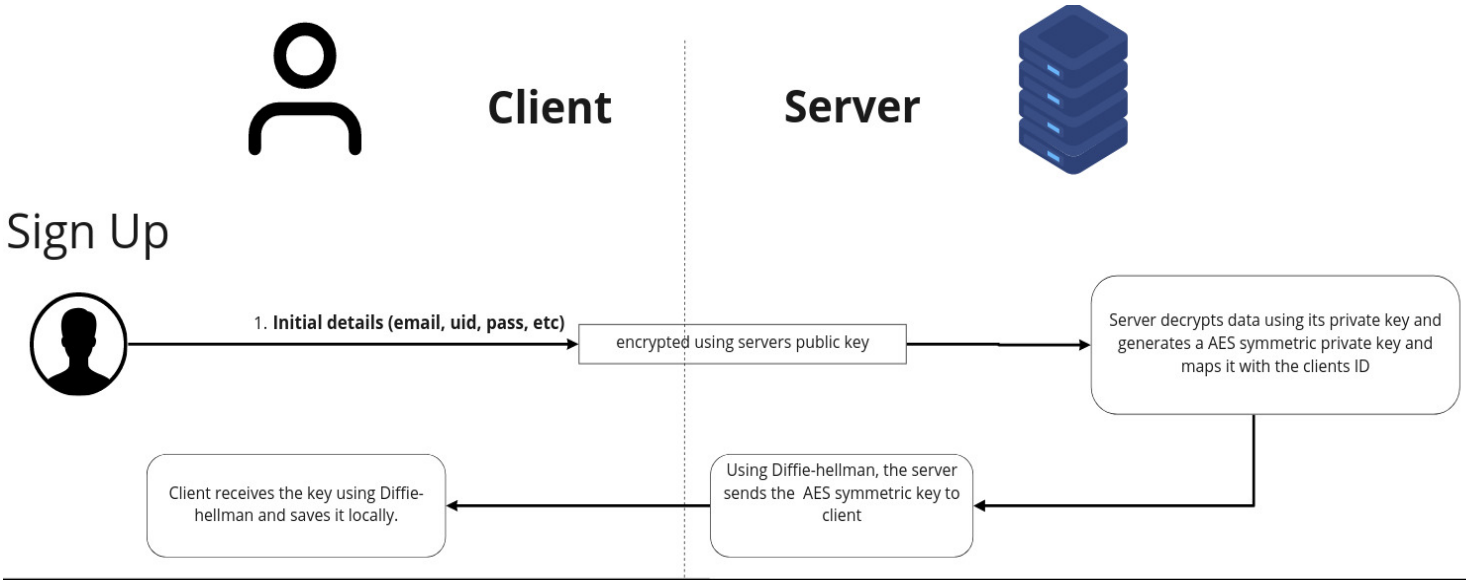
Silva and Sousa show that arrangement issues are potentially the most notable classes of specific issues that lead to the mistake of programming systems. Regardless, perceiving the arrangement issues is nontrivial.

Various assessments have reviewed the components that on a very basic level affect shopper reliability and customer commitment in web business. A couple of components like evident comfort, seen convenience, customer risk wisdom, customer care, customer trust, progression, information quality, trade security, web structure, and brand image of online business sway satisfaction when shopping on an electronic business webpage and out and out influences customer resolve. Khalid surmised that electronic business organization quality (particularly related to security and portion methodology) is the focal segment impacting buyer steadfastness with online business structure.Tabaei found features and webpage quality as key segments for electronic shopper dedication. They assume that quality estimations to the extent of accommodation, web piece, responsiveness, customization and assertion, among various segments, have positive relationships with buyer dedication and trust. Cao recognized, reviewed, and facilitated four courses of action of segments (structure quality, information quality, organization quality, and allure) that get online business webpage quality using the TAM model. They give valuable standards to online business bosses and site trained professionals. Their result maintains the circumstance of Chakraborty in the examination of heralds of site sufficiency.

Gelard and Negahdari say that different web unequivocal components including course, interface and altered substance and update are essential parts in online business structures progression. Marszałkowski explored the store time factor in web searcher situating which is major for advancing plans of various e-associations and they show that the pile time factor expects a basic part in the situating of recorded records. Vollset recognized page stacking time as one of the huge complaints by web business webpage customers. The speed of a page unfavorably impacts a customer's gathering significance, thus a site page speed impacts a seller's pay since stacking speed is a huge ally of page surrender. All the more sluggish page response times achieve a development in page surrender.

4. Proposed method

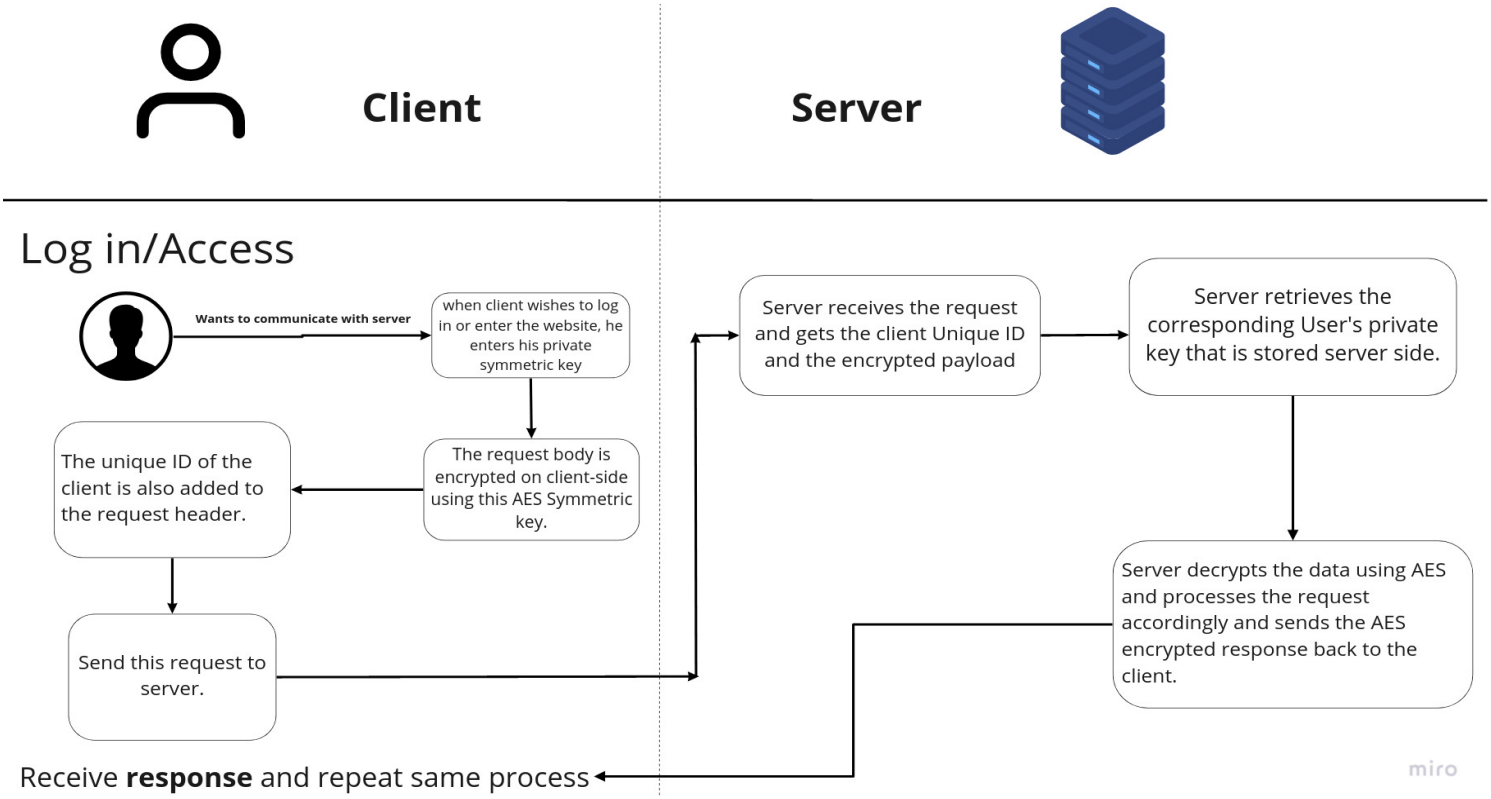
The diagram shows the complete security flow of the proposed architecture



A. **Sign Up Process:**

1. Initially we will have a public key pair on client and server. Client will hold the public key and the server will hold the private key. This will be to ensure encryption of data at the initial stage. These keys will be changed periodically with a cron job to reduce attacks by cryptanalysis.
2. The user will first enter his details and click on the signup button, then the encryption flow will start where the body of the form that has been submitted will be encrypted.
   Eg. req.body = RSA(req.body, publicKey)
3. Now this encrypted payload will be sent back to the server. This data seems random hence cannot be interpreted even if someone intercepts the network.
4. Once the server receives the data, the server will decrypt this data with the private key that was held by the server initially.
5. Server further processes the data, creates an account and stores the information about the user in the database.
6. Now the server randomly generates a symmetric private key, something like AES algorithm and maps this Symmetric Private Key to the Unique ID given to the user.. This key is sent as a successful response to the account creation. This Private Symmetric Key will be later used in further interactions of the user with the platform.
7. The key is sent with the Diffie-Hellman Key Exchange Protocol to the client so no one would listen to it.

8. Once a client receives the key, they will be asked to save it locally and safely with them as this key will be needed to enter whenever the user opens the website later.



B. **Log in and further communication**

1. Now when the user opens the website, they will be asked to enter the private key that was received during the signup. This Symmetric Private key will be used to encrypt the data being sent to the server.
2. When a user logs in, this Symmetric Private key is used to encrypt the request body to the client, the unique user ID or the email ID which the client will enter to login can be attached as a header to the request. As the user ID is already public, this method should not cause any problems. Now since the request has been generated completely, it is sent to the server.
3. Now the server gets the request and the server will retrieve the user ID which was attached to the request header.
4. Server now maps the user ID to get the Symmetric Private Key stored locally on the server. The Symmetric Private Key is later used to process the request further.
5. Server now decrypts the payload that was received with the request. Now this decrypted request contains the data needed to apply the business logic efficiently.

6. Now the server further processes the request and gives the required output.

7. The output is again encrypted with the Symmetric Private Key. This encrypted output is sent back to the user end device.
8. Now the user has received the required data in encrypted format. User side device will use the Symmetric Private key to again decrypt the data.
9. In this way, a secured end to end encryption is achieved between client and server.

C. **Database Security**

In an Ecommerce website the database security is very important, so to protect the database we are proposing hashing and encrypting the database whenever possible. We also suggest newer and secure algorithms like Blake2b for hashing all sensitive data.

Also we propose NoSQL as they offer better performance, scalability, availability, affordability, and flexibility to meet the above needs of the customer because NoSQL databases make managing product, order, and customer information relatively easier**.**

6 Conclusions and future work

As of late, the web brought a lot of challenges. A substitution transformation was essential. The net application model is regularly seen as a partner degree augmentation of the occasion driven model. Inside the last mentioned, clients are given a ton of choices on what activity they need, they need, they need, to perform and once they attempt to do it. Notwithstanding this relative opportunity, they don't have the determination and furthermore the area from which they execute their orders. Net applications have brought that new measurement. Clients will as of now select once, what and any place they utilize the application. The expansion of this new measurement puts stores of weight on the organization framework supporting net applications. Security is also a problem. Organization chiefs don't have the visual administration any more. Various procedures, similar to cryptography, will not ensure the personality of buyers. Web based business sites even have to have the option to bring to the table confirmation of character to online clients.

Clients' use of the web based business model to search for items or administrations is developing in much bigger environmental factors than they were in more seasoned applications. They'll be dependent upon government rules and controls. Internet business applications bring a great deal of essential style issues than the other application. Creators ought to demandly choose their improvement ways and instruments, and that they should endeavor to utilize formal ways at whatever point it's possible or required. During this article, we will in general know the critical difficulties inside the style of internet business applications and close these with online

business applications reasonableness to guarantee reasonable customer nature of client aptitude. Further, we will in general analyze the difficulties inside the style of internet business applications/frameworks to oblige the expanding refinement of online business applications and furthermore the expanding requests of clients for better caliber of client skill.

This investigation of the look issues in online business frameworks improvement manages issues that eventually affect the overall framework quality and hence the variables that affect customer fulfillment of web based business sites. Along these lines, this content has instructive and reasonable ramifications for web based business sites, the executives, plan, and execution improving. most importantly, we tend to fixated on 3 wide primary test zones:

(a) anyway advances, structures, and designs impact and cause online business applications engineers to require sure untimely and unfortunate style decisions,

(b) the intuitiveness and intricacy of internet business applications which needs designers to supply numerous models rather than one model for a comparable disadvantage, and at last

(c) effect of existing quality evaluation measures for web based business applications style.

Albeit the longitudinal investigation of difficulties in creating internet business managing frameworks gives bits of knowledge into fitting and property plan strategies for web based business dealers to help shoppers' mastery in online mode, we will in general carry out our style proposals. It very well may be educational to execute our proposals in a visual B2C web based business stage to collect exact information to evaluate the degree of the end of those difficulties/issues versus internet business applications needs and furthermore the accomplishment of the look quality objectives. We will in general resolve to expand this and add numerous headings. In the first place, we will in general want to supply a quantitative system for assessing code styles. Despite the fact that this is frequently in no way, shape or form a trifling expansion because of the intricacies concerned, such a system would work inside the direct and quick investigation of the numerous competitor styles that would be made as opposed to anticipating sense and natural standards.

Second, by setting up a plainly particular pathway that connections code style and furthermore the standard of organization security and application wellbeing and security, web based business applications stylers/engineers would approach a group of information to help them in making the legitimate plan choices in regard of organization security and application wellbeing

and security. At last, we will in general resolve to offer a portrayal of styles fitting for online business exchanges and frameworks.

Acknowledgements
We thank our teacher Prof. SATHYARAJ R for his guidance and support without whom this paper would not be possible.

References
Cyber Security; Issue and Challenges in E-Com'

E-Commerce Security Challenges: A Taxonomy

Y. Wen, C. Zhou, J. Ma and K. Liu, "Research on E-Commerce Security Issues," 2008 International Seminar on Business and Information Management, Wuhan, 2008, pp. 186-189, doi: 10.1109/ISBIM.2008.168.

The Study of E-Commerce Security Issues and Solutions
Sangeetha M K Prof. Dr. Suchitra R Jain University, Bangalore Jain University,Bangalore

Kefa Rabah , 2006. Implementing Secure RSA Cryptosystems Using Your Own Cryptographic JCE Provider. Journal of Applied Sciences, 6: 482-510.

Design and implementation of an improved RSA algorithm, Yunfei Li ; Qing Liu ; Tong Li,2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT),10.1109/EDT.2010.5496553

An approach for benchmarking the security of web service frameworks. https://doi.org/10.1016/j.future.2019.10.027

A Web Service Security Governance Approach Based on Dedicated Micro-services. https://doi.org/10.1016/j.procs.2019.09.192

Formal methods for web security. https://doi.org/10.1016/j.jlamp.2016.08.006

Web Application Security: An Investigation on Static Analysis with other Algorithms to Detect Cross Site Scripting. https://doi.org/10.1016/j.procs.2019.11.230

Measuring web service security in the era of Internet of Things. https://doi.org/10.1016/j.compeleceng.2017.06.020

Enhancing the security of patients' portals and websites by detecting malicious web crawlers using machine learning techniques. https://doi.org/10.1016/j.ijmedinf.2019.103976

The Web Security Password Authentication is based the Single-block Hash Function. https://doi.org/10.1016/j.ieri.2013.11.002

Survey on JavaScript security policies and their enforcement mechanisms in a web browser. https://doi.org/10.1016/j.jlap.2013.05.001

Web Services Security Problem in Service-oriented Architecture. https://doi.org/10.1016/j.phpro.2012.02.241

Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security. https://doi.org/10.1016/j.entcs.2014.01.024

A Kerberos security architecture for web services based instrumentation grids. https://doi.org/10.1016/j.future.2008.11.004

Assessing the security of web service frameworks against Denial of Service attacks. https://doi.org/10.1016/j.jss.2015.07.006

Tracing known security vulnerabilities in software repositories – A Semantic Web enabled modeling approach. https://doi.org/10.1016/j.scico.2016.01.005

Semantic security against web application attacks. https://doi.org/10.1016/j.ins.2013.08.007

A lightweight web-based vulnerability scanner for small-scale computer network security assessment. https://doi.org/10.1016/j.jnca.2008.04.007

Security Busters: Web browser security vs. rogue sites. https://doi.org/10.1016/j.cose.2015.04.009

V. Mainanwal, M. Gupta and S. K. Upadhayay, "Zero Knowledge Protocol with RSA Cryptography Algorithm for Authentication in Web Browser Login System (Z-RSA)," 2015 Fifth International Conference on Communication Systems and Network Technologies, 2015, pp. 776-780, doi:10.1109/CSNT.2015.90.

S. Beniwal, Ekta and Savita, "An effective efficiency analysis of Random Key Cryptography over RSA," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 2015, pp. 267-271.

Liang Wang and Yonggui Zhang, "A new personal information protection approach based on RSA cryptography," 2011 IEEE International Symposium on IT in Medicine and Education, 2011, pp. 591-593, doi: 10.1109/ITiME.2011.6130907.

S. Sharma, P. Sharma and R. S. Dhakar, "RSA algorithm using modified subset sum cryptosystem," 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), 2011,pp. 457-461, doi: 10.1109/ICCCT.2011.6075138.

R. S. Dhakar, A. K. Gupta and P. Sharma, "Modified RSA Encryption Algorithm (MREA)," 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012, pp.426-429, doi: 10.1109/ACCT.2012.74.

Qing Liu, Yunfei Li, Lin Hao and Hua Peng, "Two efficient variants of the RSA cryptosystem," 2010 International Conference On Computer Design and Applications, 2010, pp. V5-550-V5-553, doi:10.1109/ICCDA.2010.5541133.

K. Balasubramanian, "Variants of RSA and their cryptanalysis," 2014 International Conference on Communication and Network Technologies, 2014, pp. 145-149, doi: 10.1109/CNT.2014.7062742.

N.M. S. Iswari, "Key generation algorithm design combination of RSA and ElGamal algorithm," 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 2016, pp. 1-5, doi: 10.1109/ICITEED.2016.7863255.

P. Ora and P. R. Pal, "Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography," 2015 International Conference on Computer, Communication and
Control (IC4), 2015, pp. 1-6, doi: 10.1109/IC4.2015.7375655.

W. Geiselmann and R. Steinwandt, "Special-Purpose Hardware in Cryptanalysis: The Case of 1,024-Bit RSA," in IEEE Security & Privacy, vol. 5, no. 1, pp. 63-66, Jan.-Feb. 2007, doi: 10.1109/MSP.2007.20.

H. Sun, M. Wu, W. Ting and M. J. Hinek, "Dual RSA and Its Security Analysis," in IEEE Transactions on Information Theory, vol. 53, no. 8, pp. 2922-2933, Aug. 2007, doi: 10.1109/TIT.2007.901248.

R. Minni, K. Sultania, S. Mishra and D. R. Vincent, "An algorithm to enhance security in RSA," 2013
Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-4, doi: 10.1109/ICCCNT.2013.6726517.

B. R. Ambedkar, A. Gupta, P. Gautam and S. S. Bedi, "An Efficient Method to Factorize the RSA Public Key Encryption," 2011 International Conference on Communication Systems and Network
Technologies, 2011, pp. 108-111, doi: 10.1109/CSNT.2011.29.

R. Patidar and R. Bhartiya, "Modified RSA cryptosystem based on of line storage and prime

number," 2013 IEEE International Conference on Computational Intelligence and Computing Research,
2013, pp. 1-6, doi: 10.1109/ICCIC.2013.6724176.

A. Karakra and A. Alsadeh, "A-RSA: Augmented RSA," 2016 SAI Computing Conference (SAI), 2016, pp. 1016-1023, doi: 10.1109/SAI.2016.7556103.

Larman C. Applying UML and Patterns: an Introduction to Object Oriented Analysis and Design and Iterative Development. 3rd ed. Upper Saddle River, NJ: Prentice Hall PTR; 2004.

Brunet J, Murphy GC, Terra R, Figueiredo J, Serey D. Do Developers Discuss Design? Proceedings of the 11th Working Conference on Mining Software Repositories (MSR 2014), New York, NY:340-343.

Bourque P, Fairley RE(D), eds. SWEBOK Guide V3.0: Guide to the Software Engineering Body of Knowledge. Washington, DC: IEEE Computer Society; 2014.

Hummel O, Eichelberger H, Giloj A, Werle D, Schmid K. A Collection of Software Engineering Challenges for Big Data System Development. Euromicro SEAA 2018 in Prague, IEEE; 2018.

Sousa L, Oliveira R, Garcia A, et al. How Do Software Developers Identify Design Problems? Proceedings of 31st Brazilian Symposium on Software Engineering (XXXI SBES), Fortaleza, Ceará, Brazil, September 10, 2017.

MacCormack A, Rusnak J, Baldwin C. Exploring the structure of complex software designs: an empirical study of open source and proprietary code. Manag Sci. 2006;52(7):1015-1030.

van Gurp J, Bosch J. Design erosion: problems and causes. J Syst Software. 2002;61(2):105-119.

Silva MCO, Valente MT, Terra R. Does Technical Debt Lead to the Rejection of Pull Requests? Proceedings of the 12th Brazilian Symposium on Information Systems (SBSI'16); 2016:248-254.

Xiao L, Cai Y, Kazman R, Mo R, Feng Q. Identifying and Quantifying Architectural Debt. Proceedings of the 38th International Conference on Software Engineering (ICSE '16), ACM, New York, NY; 2016:488-498.

Sousa L, Oliveira A, Oizumi W, et al. 2018. Identifying Design Problems in the Source Code: A Grounded Theory. In ICSE '18: 40th International Conference on Software Engineering. May 27-June 3, 2018, Gothenburg, Sweden. ACM, New York, NY; 14.

Garcia J, Popescu D, Edwards G, Medvidovic N. Identifying Architectural Bad Smells. Proceedings of the 2009 European Conference on Software Maintenance and Reengineering (CSMR '09); March 24-27, 2009, Kaiserslautern, Germany: IEEE Computer Society, Washington, DC; 2009:255-258.