IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022 ISSN: 2320-1363

Design and Implementation of Secure Web Application using SSLALG

1. A.N.Mamatha, 2.R.Prabhakar Naidu(Ph.D)

1.MCA, Mother Theresa Institute of Computer Applications, Palamaner, S.V.University, Tirupathi, A.p, India.

2.AsstProf, Mother Theresa Institute of Computer Applications, Palamaner, S.V.University, Tirupathi,A.p, India.

anmamatha1999@gmail.com,

mtimca@gmail.com

Abstract: SSL is one of the most well-known conventions utilized on the Internet for secure correspondences. Anyway SSL convention has a few issues. In the first place, SSL convention carries extensive weight to the CPU use so execution and speed of the security administration is brought down during encryption exchange. Second, SSL convention can be powerless for cryptanalysis because of the fixed calculation being utilized. Third, it causes an issue of common association with different conventions in view of the encryption send out limitation strategy of the U.S. Fourth, it is hard for designers to learn and utilize cryptography API for SSL. To take care of these issues, right now, propose a SSL segment dependent on CBD. The execution of the SSL segment is upheld by Confidentiality and Integrity part. It can encode information specifically and utilize different instruments, for example, SEED and HAS-160. Likewise, it can supplement the SSL protocol. issues and, simultaneously, exploit segment. At long last, in the exhibition investigation, we present a superior outcome than the SSL convention as the information size is expanded.

I. Introduction: As of late, SSL convention has been predominantly utilized as a security convention for secure correspondences over the Internet with OpenSSL by Eric A. Youthful, JSSE (java secure attachment expansion) by Sun Microsystems, and so on. While SSL is the most well-known and broadly utilized convention between internet browsers and web servers [1], it has a few issues: First, SSL convention carries significant weight to the CPU usage with the

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022 ISSN: 2320-1363

goal that presentation of the security administration in encryption exchange is brought down in light of the fact that it scrambles all information which is moved among server and client [2]. Second, SSL convention can be powerless for cryptanalysis because of the fixed calculation being utilized. Along these lines, engineer can't utilize different instruments, for example, SEED and HAS-160. Third, it causes an issue of shared communication with different conventions because of the encryption trade limitation approach of the U.S[4]. At long last, it is hard for designers to learn and utilize cryptography API (application program interface) for SSL. Subsequently, we need another technique which is not quite the same as the current one to utilize SSL convention all the more effectively in plan and execution of uses. Right now, propose a SSL segment dependent on CBD so as to take care of the issues referenced previously. The segment is actualized on the application level where it can encode and decode information. Clients can pick different calculations of encryption. The SSL part gives comfort to the engineers who are not familiar with security ideas. It can likewise effectively furnish SSL administrations when interlocked with different business segments in view of its part based execution. The SSL part is reusable and expands the profitability and it diminishes the cost [5]. Likewise, as segment engineers need stage autonomous strategies to help their advancements paying little heed to platform cryptography APIs, it can bolster the segment stage freely regardless of the sort of subordinate encryption APIs. Thus, the segment makes it simple to connect and interlink between conventions. Right now, propose the prerequisites for SSL segment and structure it dependent on CBD. We have executed inside SSL handshake convention and SSL record convention so as to play out similar elements of the current SSL usage. Further, we planned the primary security segment – Integrity and Confidentiality administration segment – that underpins the piece of SSL part. Here, we include standard calculations utilized in Korea for cryptography, for example, SEED and HAS-160[7] and engineers utilizing the segment can choose the calculation type and encoding/unraveling type. As such, we give assortment

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022 ISSN: 2320-1363

cryptography components of SSL and usage to encode/decode information specifically, in this manner rendering information preparing to be progressively productive. We utilized the Rational Rose 2000 as a plan instrument for the part and arrangement diagram [8], and executed the SSL, Confidentiality and Integrity segment with EJB [9]. Ultimately, we tried the usage of every segment with the fitting situation for SSL segment and J2EE [10] server as indicated by our proposed plan. We additionally tried the effectiveness against the standard SSL convention. The rest of this paper is sorted out as follows. Section 2 clarifies the investigation of necessities for SSL segment and presents the proposed plan of SSL segment, which takes care of the previously mentioned issues. Section 3 presents the usage of SSL and the primary security part as indicated by the structure of Chapter 2, and afterward gives the test through the best possible situation. Further, execution assessment results contrasted and SSL convention are introduced in Chapter 3. At long last, Chapter 4 finishes up the paper with a short conversation on the future work.

II. Objective: The fundamental target of this undertaking is to send the classified subtleties and related secret records and reports to their beneficiaries in a securable manner. Cryptology for Security will utilize the various sorts of calculations to create the encoded strings, documents and decoded strings, records. The Secure Sockets Layer (SSL) is a typical Encryption convention utilized in Cryptolog. At the point when you see a URL in your Web program that begins with "https" rather than "http", it is a protected association that is utilizing SSL.Some techniques for cryptography utilized a "mystery key" to permit the beneficiary to decode the message. The most widely recognized mystery key cryptosystem is the Data Encryption Standard (DES), or the more secure Triple-DES which scrambles the information multiple times. The deliberate calculations utilized by Cryptolog will be in the types of:

1. MD5
2. SHA1
3. Rijndael Managed

III. Existing System:

1) In Existing framework, the information will be secure through the system since

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022 ISSN: 2320-1363

information transmission is done in scrambled organization.

2) In Existing framework, information won't be gotten to through the approved individual.

3) The framework doesn't give security to the information store in database.

4) In Existing System, the security isn't given all through the server and database.

IV. Proposed System:

1) In Proposed System, the information will be secure utilizing the web innovation by utilizing https empowered.

2) In Proposed System, the information will be gotten to through the approved individual.

3) The framework gives security to the information store in the database.

4) In Proposed System, the security is given all through the server and database by crippling the treats and so on.

The Cryptology has been isolated into 5 distinct modules:

1. Executive
2. Client
3. Mysterious messages
4. Mysterious records
5. Picture change

Executive: Executive is a super client in the framework. He will screen all the clients' exercises in the framework. He has benefits to do anything anytime of time. He is liable for giving secure component to the client of the framework to send their private information in a safe manner. (not obvious)

Client: Client will enlist in to site and send his private information in a made sure about path by utilizing Crypto log innovation office gave in the application.

Obscure messages: Right now, will send his private messages in an encryption group with the goal that recipient will get the information and he will unscramble to get unique information. With the goal that information will transmitted in a protected manner.

Mysterious documents: Right now, will send information document in an encryption group with the goal that beneficiary will get the information and he will unscramble to get unique information. Application gives an office to send records in a made sure about way.

Picture change: Right now will transmit information as picture and he can scramble the picture and change to beneficiary.

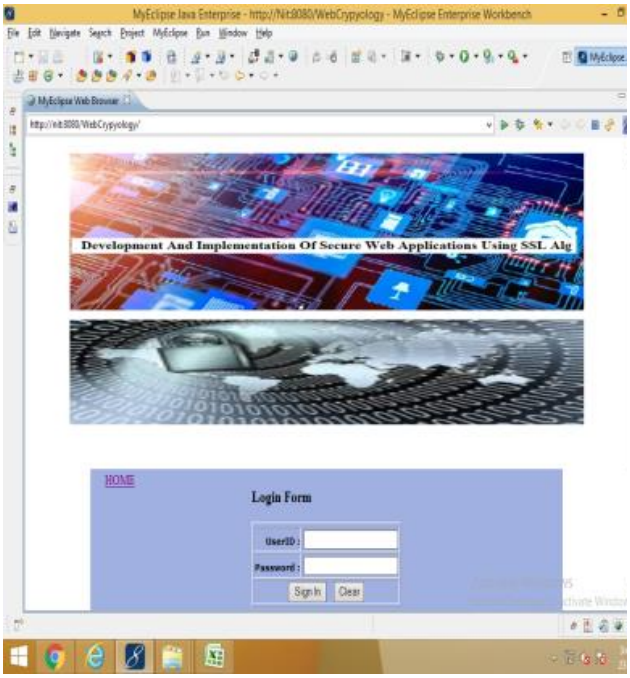
IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022

ISSN: 2320-1363

Recipient will get the information and he will unscramble to get unique information. By utilizing this application client can send pictures additionally in a made sure about way.

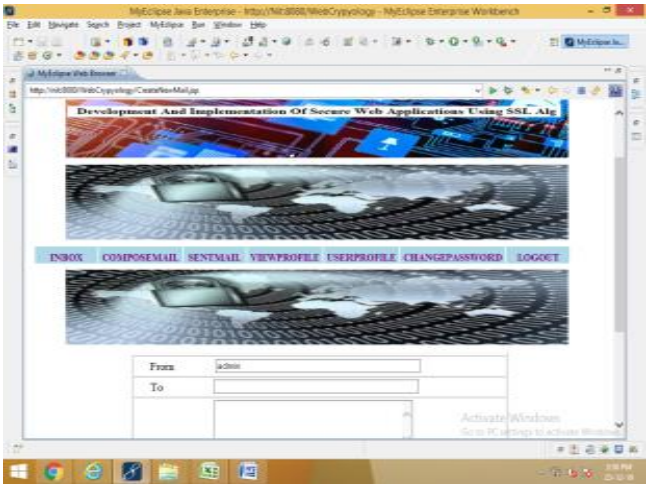
V. Experimental Results

Home page



Admin login page

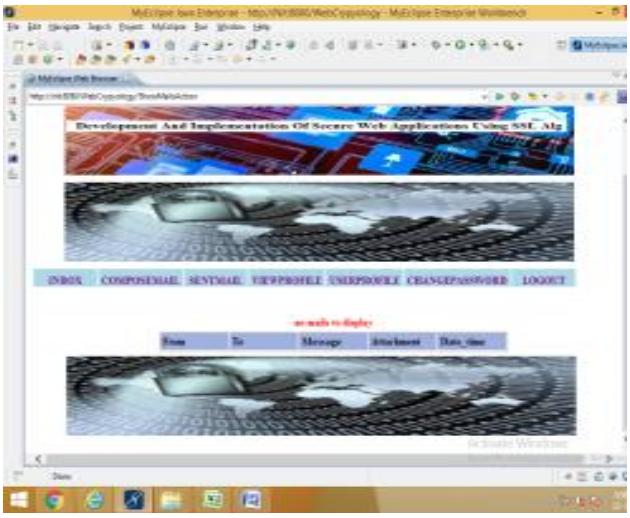
Admin compose mail



Admin check sent mail info

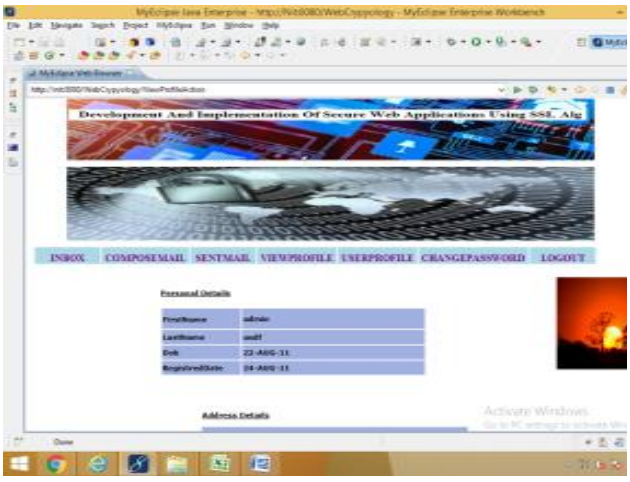
IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022

ISSN: 2320-1363

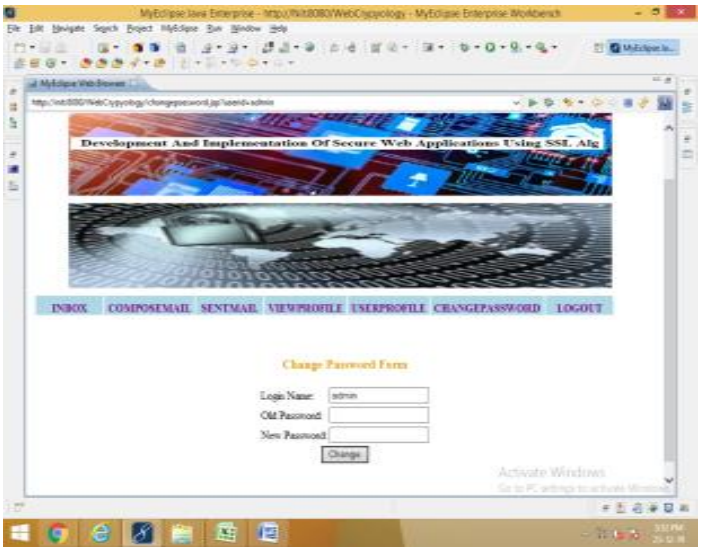


Admin check view profile

Admin check change password



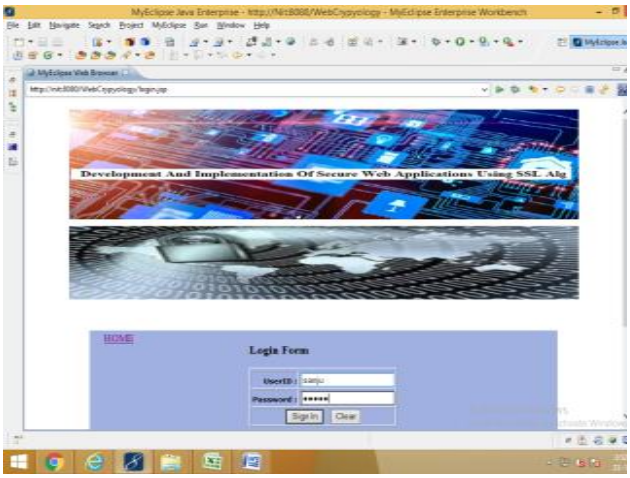
Admin check user profile



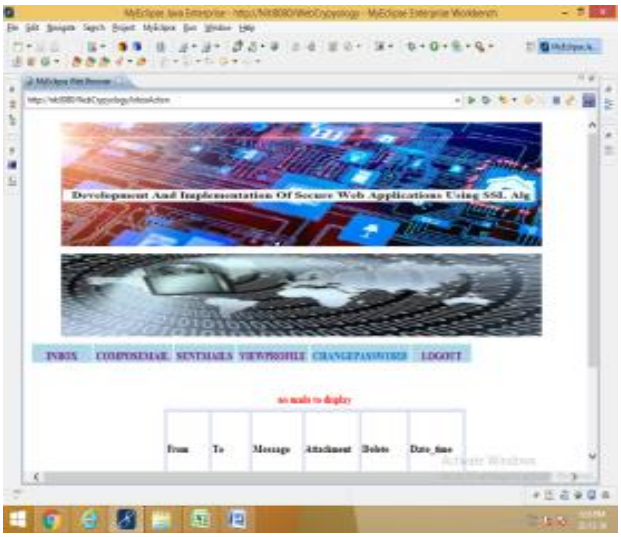
User login page

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022

ISSN: 2320-1363

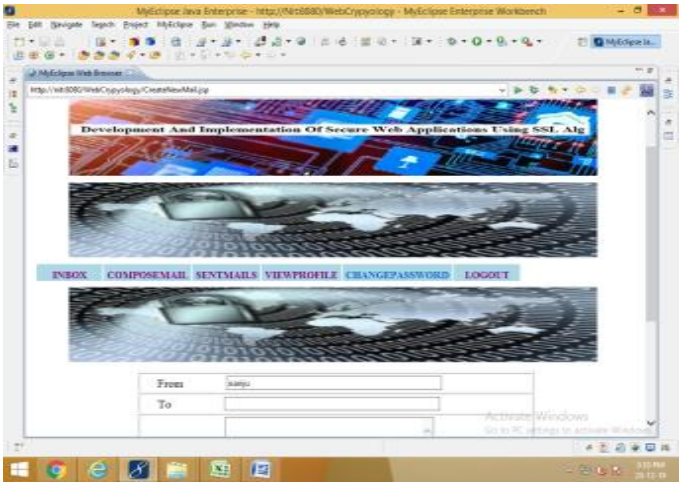


User home page



User compose mail

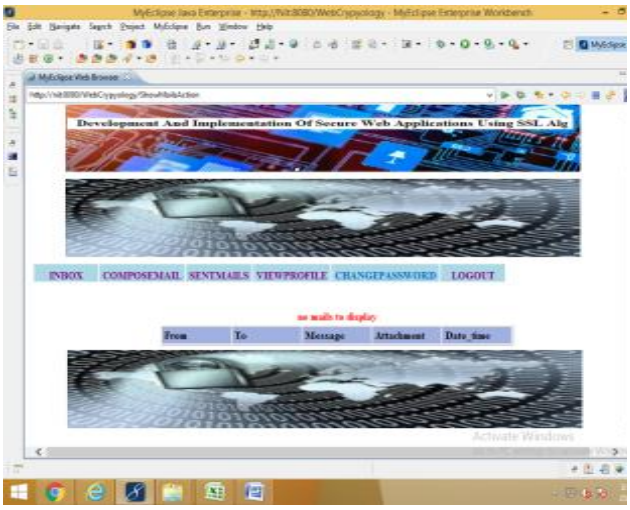
User inbox mail



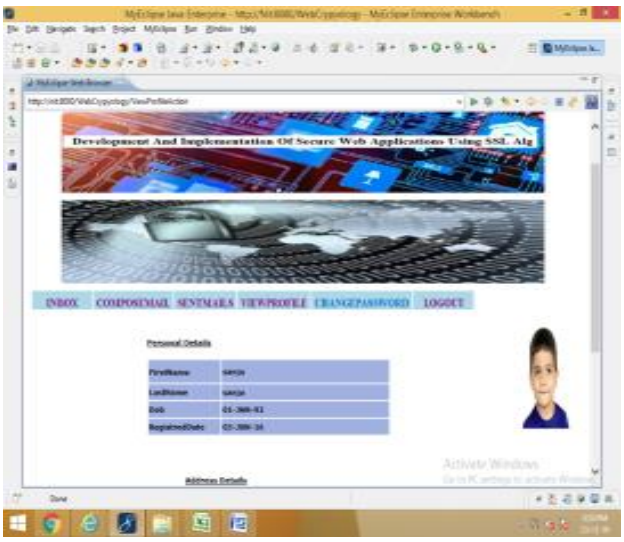
User send mail

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022

ISSN: 2320-1363



User view profile



VI. Conclusion and Future Work: Right now, proposed and executed the model to give the SSL administration through the framework dependent on CBD. SSL Component model dependent on CBD expands the current SSL convention using halfway message encryption and Korean local standard cryptography calculations which wasn't gave in the current SSL convention. We additionally conquered the confinement of SSL protocol through the product improvement which has the part idea. The SSL Component can be reused, scrambled specifically, applied for Korean local standard calculation and it very well may be expanded. As appeared in the part 3, when the size of information turns out to be little we can decrease the requirement for CPU assets by utilizing the remote association of a segment. Then again, when the information volume size is expanded, proposed SSL Component turns out to be increasingly proficient, since it can scramble the chose information dependent on CBD. Right now, utilized mysterious Diffie-Hellman calculation, which is very basic. With respect to future work, we have to propose and plan the perplexing validation part more plainly. Further, we have to present and actualize the standard for the segment that would give other security administrations, for example, non-notoriety and accessibility.

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022 ISSN: 2320-1363

References:

[1]. William Stallings: Cryptography and Network Security. Standards and Practice, third edn, Prentice Hall (2002)

[2]. R. W. Badlwin et C. V. Chang: Locking the e-safe. IEEE Spectrum (1997)

[3]. A. Freier, P Karlton, and P. Kocher: The SSL Protocol Version 3.0, Internet Draft (1996)

[4]. Xiaodong Lin, Johnny W. Wong, Weidong Kou: Performance Analysis of Secure Web Server Based on SSL. Talk Notes in Computer Science, Springer-Verlag Heidelberg, Volume 1975/2000, Information Security: Third International Workshop, ISW 2000, Wollongong, Australia, December 2000. Procedures (2003) 249-261

[5]. K. Kant, R. Iyer and P. Mohapatra: Architectural Impact of Secure Socket Layer on Internet Servers. Proc. IEEE 2000 International Conference on Computer Design (2000) 7-14

[6]. Kyoung-gu, Lee: TLS Standard Trend. KISA, The updates on Information Security, vol. 19(1999)

[7]. Chris Frye: Understanding Components. Andersen Consulting Knowledge Xchange (1998)

[8]. KISA: SEED Algorithm Specification. Korea Information Security Agency (1999)

[9]. TTA Standard: Hash Function Standard-Part 2: Hash Function Algorithm Standard (HAS-160). Broadcast communications Technology Association (2000)

[10]. Booch, G., Rumbaugh, J., and Jacobson, I.: The Unified Modeling Language User Guide.Addison Wesley Longman (1999)

[11]. Endeavor Java Beans Specification Version 2.0 Final Release. Sun Microsystems Inc (2001)

[12]. Sun, Java 2 Platform Enterprise Edition Specification, Version 1.4, Sun Microsystems Inc (2004)

About Authors:

About Author:1

A.N.Mamatha is currently pursuing her Mca in Mother Theresa Institute of Computer Applications, Palamaner, Affliated to S.V University, Tirupathi. Her area of interest is computer networks.

IJMTARC – VOLUME – IX – ISSUE – 37, JAN - MAR, 2022

ISSN: 2320-1363

About Author:2

R.Prabhakar Naidu (Ph.D) He is currently working as a HOD& Associate Professor in Mother Theresa Institute of Computer Applications, Palamaner with total experience interface and of 20 years, as a test engineer for 4 years,16years of teaching in computer science. His areas of interest are computer security, Operating Systems and Software Engineering