PENGAMANAN PESAN TEKS BERBASIS *END-TO-END ENCRYPTION* MENGGUNAKAN ALGORITMA AES 256 BIT DAN ECDH

Diajukan Sebagai Syarat untuk Menyelesaikan

Pendidikan Program Strata-1 pada

Jurusan Teknik Informatika

Oleh:

Nabiel Omar Syarif

NIM: 09021182025031

Jurusan Teknik Informatika

FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

PENGAMANAN PESAN TEKS BERBASIS END-TO-END ENCRYPTION MENGGUNAKAN ALGORITMA AES 256 BIT DAN ECDH

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Teknik Informatika

Oleh:

NABIEL OMAR SYARIF

09021182025031

Pembimbing 1	**:**	**Osvari Arsalan, M.T.**
		NIP. 198806282018031001
Pembimbing 2	**:**	**Dr. Annisa Darmawahyuni, M.Kom.**
		NIP. 199006302023212044

Mengetahui

Ketua Jurusan Teknik Informatika

Hadipurnawan Satria, Ph.D

198004182020121001

TANDA LULUS UJIAN KOMPREHENSIF

Pada hari Jum'at tanggal 28 Februari 2025 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	: Nabiel Omar Syarif
NIM	: 09021182025031
Judul	: Pengamanan Pesan Teks Berbasis *End-To-End Encryption* Menggunakan Algoritma AES 256 Bit dan ECDH

dan dinyatakan **LULUS**

1. Ketua Penguji

   Dr. Muhammad Fachrurrozi, M.T. .....
   NIP. 198005222008121002

2. Penguji

   Julian Supardi, M.T., Ph.D. .....
   NIP. 197207102010121001

3. Pembimbing I

   Osvari Arsalan, M.T. .....
   NIP. 198806282018031001

4. Pembimbing II

   Dr. Annisa Darmawahyuni, M.Kom. .....
   NIP. 199006302023212044

Mengetahui,
Ketua Jurusan Teknik Informatika

Hadipurnawan Satria, Ph.D.
NIP. 198004182020121001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Nabiel Omar Syarif

NIM : 09021182025031

Program Studi : Teknik Informatika

Judul Skripsi : Pengamanan Pesan Teks Berbasis *End-To-End Encryption* Menggunakan Algoritma AES 256 Bit dan ECDH

Hasil pengecekan *Software* ~~*iThenticate*~~*/Turnitin* : 9%

Menyatakan bahwa laporan penelitian saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan penelitian ini, maka saya bersedia menerima sanksi akademik Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapa pun.

Palembang, 05 Maret 2025

Nabiel Omar Syarif

NIM 09021182025031

MOTTO DAN PERSEMBAHAN

"The only way to do great work is to love what you do."

— Steve Jobs

Kupersembahkan Karya Tulis ini kepada:

- Allah SWT
- Kedua orang tua dan saudara saya
- Fakultas Ilmu Komputer
- Universitas Sriwijaya

ABSTRACT

Digital communication security is critical amid growing privacy threats, particularly on instant messaging platforms vulnerable to eavesdropping. One solution to address this challenge is the use of encryption. This study aims to enhance the security of text messages through the implementation of End-to-End Encryption (E2EE) by combining the Advanced Encryption Standard (AES) 256-bit for symmetric encryption and the Elliptic Curve Diffie-Hellman (ECDH) for secure key exchange. AES was selected for its ability to provide fast and efficient encryption, while ECDH ensures secure key exchange through the mathematical complexity of elliptic curves. The results demonstrate that AES 256-bit achieves an average encryption time of 0.0196 milliseconds for text ranging from 3 to 30 characters, accompanied by an Avalanche Effect of 77%, indicating optimal ciphertext randomness. Meanwhile, ECDH successfully prevented key interception during the exchange process, and the system withstood simulated man-in-the-middle attacks. Thus, the combination of AES and ECDH proves effective as a secure and efficient E2EE solution for instant messaging applications.

Keywords : *End-to-End Encryption*, *Advanced Encryption Standard*, *Elliptic Curve Diffie-Hellman, Instant Messaging*

ABSTRAK

Keamanan komunikasi digital sangat penting di tengah ancaman privasi yang terus meningkat, terutama pada platform pesan instan yang rentan terhadap penyadapan. Satu solusi untuk mengatasi tantangan ini adalah penggunaan enkripsi. Penelitian ini bertujuan untuk meningkatkan keamanan pesan teks melalui implementasi *End-to-End Encryption* (E2EE) dengan menggabungkan *Advanced Encryption Standard* (AES) 256-bit untuk enkripsi simetris dan *Elliptic Curve Diffie-Hellman* (ECDH) untuk pertukaran kunci yang aman. AES dipilih karena kemampuannya untuk menyediakan enkripsi yang cepat dan efisien, sementara ECDH memastikan pertukaran kunci yang aman melalui kompleksitas matematis kurva elips. Hasilnya menunjukkan bahwa AES 256-bit mencapai waktu enkripsi rata-rata 0,0196 milidetik untuk teks mulai dari 3 hingga 30 karakter, disertai dengan Avalanche Effect sebesar 77%, yang mengindikasikan keacakan *ciphertext* yang optimal. Sementara itu, ECDH berhasil mencegah penyadapan kunci selama proses pertukaran, dan sistem ini tahan terhadap serangan *man-in-the-middle* yang disimulasikan. Dengan demikian, kombinasi AES dan ECDH terbukti efektif sebagai solusi E2EE yang aman dan efisien untuk aplikasi pesan instan.

Kata Kunci : *End-to-End Encryption*, *Advanced Encryption Standard*, *Elliptic Curve Diffie-Hellman, Instant Messaging*

KATA PENGANTAR

Puji dan syukur ke hadirat Allah SWT atas segala nikmat, rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi yang berjudul "Pengamanan Pesan Teks Berbasis End-To-End Encryption Menggunakan Algoritma AES 256 Bit dan ECDH". Skripsi ini disusun sebagai salah satu syarat kelulusan program Strata-1 pada Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Dalam menyelesaikan skripsi ini, penulis menerima banyak bantuan, bimbingan serta dukungan dari banyak pihak, baik secara langsung maupun secara tidak langsung. Oleh karena itu, penulis ingin menyampaikan terima kasih kepada:

1. Allah SWT atas semua rahmat dan nikmat-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
2. Orang tua beserta keluarga besar yang selalu memberikan dukungan, bantuan, doa, serta motivasi untuk menyelesaikan skripsi ini.
3. Bapak Prof. Dr. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Hadipurnawan Satria, Ph.D. selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Osvari Arsalan, M.T. dan Ibu Dr. Annisa Darmawahyuni, M.Kom. selaku dosen pembimbing penulis dalam menyelesaikan skripsi ini.
6. Seluruh Dosen, Admin dan Staf Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

7. Teman-teman seperjuangan yang telah banyak membantu penulis dalam menyelesaikan skripsi ini.
8. Pihak-pihak lain yang tidak dapat disebutkan satu-persatu.

Penulis menyadari bahwa masih banyak sekali kekurangan dalam penyusunan skripsi ini dikarenakan kurangnya pengalaman serta pengetahuan penulis. Oleh karena itu, penulis sangat mengharapkan kritik dan saran agar dapat memperbaiki kesalahan dan kekurangan pada penelitian-penelitian selanjutnya. Semoga skripsi yang disusun penulis dapat membawa manfaat bagi pembacanya. Terima kasih.

Inderalaya, 05 Maret 2025

Penulis

Nabiel Omar Syarif

DAFTAR ISI

Halaman

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab ini mengupas latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan. Selain itu, dalam bab ini akan dijelaskan secara menyeluruh mengenai gambaran umum dari seluruh kegiatan penelitian yang dilakukan.

1.2 Latar Belakang Masalah

Penggunaan aplikasi pesan berbasis teks telah menjadi bagian integral dalam komunikasi sehari-hari, terutama dengan kemajuan teknologi informasi. Seiring meningkatnya kejahatan siber, seperti penyadapan dan pencurian data, diperlukan teknologi enkripsi yang lebih aman dan efisien. Pesan teks yang tidak dienkripsi rentan terhadap ancaman peretasan dan penyadapan oleh pihak yang tidak bertanggung jawab, mendorong kebutuhan akan sistem pengamanan data yang tahan terhadap berbagai serangan siber (Vichare et al., 2017).

End-to-End Encryption (*E2EE*) diperkenalkan sebagai solusi untuk mengatasi risiko tersebut dengan mengenkripsi pesan, memastikan hanya pengirim dan penerima yang dapat mengakses isi pesan. Namun, E2EE hanya melindungi pesan saat pengiriman, tidak mengamankan pesan setelah didekripsi pada sisi penerima. Untuk mengatasi potensi risiko ini, diperlukan penghapusan otomatis terhadap pesan yang dikirim, dikenal sebagai *self-message-destructing*.

Penghapusan otomatis dapat diimplementasikan dengan menggunakan parameter waktu yang dapat disesuaikan oleh pengguna, memastikan pesan terhapus setelah batas waktu tertentu.

Dalam pengembangan keamanan pesan, algoritma *Elliptic Curve Diffie-Hellman* (ECDH) dan *Advanced Encryption Standard* (AES) menjadi fokus. ECDH dikenal akan kemampuannya menghasilkan kunci bersama yang aman dan efisien untuk pertukaran kunci (Abusukhon et al., 2019), sementara AES dikenal sebagai algoritma enkripsi simetris yang cepat dan aman (Tsai et al., 2018).

Penelitian oleh Tung et al. (2012) menggunakan metode RSA dan AES untuk melindungi pengiriman pesan pada *instant messaging* dengan kemampuan *Self-Message-Destructing*. Temuan mereka menunjukkan bahwa enkripsi dan dekripsi tidak signifikan mempengaruhi kinerja aplikasi untuk pesan berukuran kurang dari 32 Kilobyte. Rihan et al. (2015) membandingkan AES dan DES diimplementasikan pada perangkat keras desktop Core i5, menunjukkan bahwa AES memberikan kecepatan enkripsi lebih tinggi dengan penggunaan CPU yang efisien dibandingkan dengan DES. Penelitian lain oleh Nugroho dan Munir (2015) menginvestigasi kriptografi dengan metode ECC untuk meningkatkan keamanan pesan pada aplikasi *instant messaging*, dengan peningkatan *overhead* seiring bertambahnya ukuran pesan.

Namun demikian, masih belum banyak penelitian yang menjelaskan bagaimana membangun sistem berbasis *End-To-End Encryption* dengan mengkombinasikan algoritma AES 256-bit dan ECDH. Salah satu penelitian terkait

yang dilakukan oleh Nugroho dan Munir (2015) hanya membahas komparasi kombinasi algoritma AES dan RSA dengan ECC, tanpa melibatkan metode *End-To-End Encryption.* Oleh karena itu, penelitian ini berfokus pada upaya dalam mengamankan pesan teks menggunakan algoritma AES dan ECDH dengan metode *End-To-End Encryption.*

Berdasarkan penjelasan di atas, Algoritma ECDH dan AES memiliki kelebihan dalam mengamankan pesan berbasis teks dengan efisien. ECDH menonjol dalam pertukaran kunci yang aman, sementara AES menawarkan enkripsi simetris yang cepat. Penggunaan *self-message-destructing* dan implementasi *E2EE* menjadi solusi efektif tanpa signifikan mempengaruhi kinerja aplikasi, sementara penelitian menunjukkan peningkatan keamanan dengan menggunakan *Elliptic Curve Cryptography* (ECC). Perbandingan dengan DES menegaskan bahwa AES memberikan kecepatan enkripsi lebih tinggi dengan penggunaan CPU yang efisien dalam melindungi pesan berbasis teks.

Oleh karena itu, penelitian ini bertujuan untuk menggabungkan kombinasi antara algoritma ECDH sebagai algoritma pertukaran kunci yang aman dan efisien, serta algoritma AES 256 bit untuk mengenkripsi pesan secara aman dan cepat. Dengan pendekatan ini, diharapkan dapat meningkatkan keamanan komunikasi pesan teks dan melindungi data dari potensi ancaman siber.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, maka adapun rumusan masalah yang dapat disimpulkan pada penelitian ini adalah sebagai berikut:

1. Bagaimana meningkatkan tingkat keamanan pesan teks melalui penerapan metode *End-to-End encryption* dengan menggunakan kombinasi algoritma *Advanced Encryption Standard* (AES) *dan Elliptic Curve Diffie–Hellman* (ECDH)?
2. Bagaimana kinerja algoritma *Advanced Encryption Standard* (AES) dalam memberikan enkripsi simetris yang cepat dan efisien?
3. Bagaimana kontribusi algoritma *Elliptic Curve Diffie–Hellman* (ECDH) dalam menciptakan pertukaran kunci yang aman pada konteks *End-to-End encryption* untuk pesan teks?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui cara meningkatkan keamanan pesan melalui penerapan metode *End-to-End Encryption* dengan menggunakan kombinasi algoritma *Advanced Encryption Standard* (AES) dan *Elliptic Curve Diffie-Hellman* (ECDH)
2. Mengetahui kinerja dari algoritma AES dalam memberikan enkripsi simetris yang cepat dan efisien
3. Mengetahui kontribusi algoritma *Elliptic Curve Diffie–Hellman* (ECDH) dalam menciptakan pertukaran kunci yang aman pada konteks *End-to-End encryption* untuk pesan teks

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah sebagai berikut :

1. Sistem yang dibuat meningkatkan keamanan pesan teks melalui *End-to-End Encryption* dengan AES dan ECDH.
2. Memanfaatkan AES untuk enkripsi efisien dan ECDH untuk pertukaran kunci aman pada *End-to-End encryption*.
3. Hasil penelitian dapat dijadikan panduan untuk pengembangan perangkat lunak *Instant Messaging* yang lebih aman pada platform *mobile* seperti Android atau IOS.

1.6 Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah sebagai berikut :

1. Sistem yang dihasilkan hanya berfokus pada pengamanan pesan, sehingga tidak menyediakan pencadangan, sinkronisasi serta restorasi pesan antar perangkat pengguna
2. Pertukaran pesan dapat terjadi hanya ketika pengirim dan penerima sedang aktif pada sistem
3. Sistem tidak menjamin ancaman keamanan yang disebabkan kelalaian pengguna dan keamanan pengaksesan data yang dilakukan secara fisik terhadap perangkat pengguna

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini telah ditetapkan sesuai standar Fakultas Ilmu Komputer Universitas Sriwijaya sebagai berikut :

BAB I. PENDAHULUAN

Bab ini menguraikan konsep dan ide pokok yang menjadi landasan penelitian, meliputi penjelasan latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian, pembatasan masalah, dan tata cara penyusunan.

BAB II. KAJIAN LITERATUR

Bab ini memberikan penjelasan mengenai dasar-dasar teori yang diterapkan dalam penelitian, beserta studi-studi lain yang relevan dengan konteks penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab ini memberikan penjelasan terperinci tentang analisis dan langkah-langkah yang ditempuh selama perjalanan penelitian, sesuai dengan kerangka kerja yang telah ditetapkan. Isi dari bab ini melibatkan aspek-aspek seperti pengumpulan data, analisis data, dan perancangan manajemen proyek.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab empat menganalisis dan membahas pengembangan *software* mengenai analisis kebutuhan dan desain pada *software*, hingga pembuatan dan pengujian *software.*

BAB V. HASIL DAN ANALISA PENELITIAN

Bab ini mengupas dan menjelaskan tentang output dari uji coba yang dilaksanakan, berdasarkan pada langkah-langkah dan proses yang sudah

ditetapkan sebelumnya. Hasil uji coba tersebut akan diuraikan sebagai dasar untuk menyusun kesimpulan.

BAB VI. KESIMPULAN DAN SARAN

Bab ini melibatkan penjelasan menyeluruh yang telah diuraikan pada bab-bab sebelumnya. Bab ini bertujuan menghasilkan kesimpulan dan saran yang diharapkan dapat membantu dalam pengembangan dan peningkatan penelitian berikutnya.

1.8 Kesimpulan

Kesimpulan yang diperoleh dari pendahuluan ini mencakup gambaran secara umum tentang pengamanan pesan teks berbasis E2EE menggunakan algoritma AES dan ECDH. Pembahasan melibatkan aspek-aspek seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan terkait dengan implementasi keamanan komunikasi pesan pada aplikasi yang dijelaskan.

DAFTAR PUSTAKA

Abusukhon, A., Mohammad, Z., & Al-Thaher, A. (2019). Efficient and Secure Key Exchange Protocol Based on Elliptic Curve and Security Models. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 73–78. https://doi.org/10.1109/JEEIT.2019.8717496

Adomnicai, A., & Peyrin, T. (2020). Fixslicing AES-like Ciphers: New bitsliced AES speed records on ARM-Cortex M and RISC-V. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2021*, 402–425. https://doi.org/10.46586/tches.v2021.i1.402-425

Bernstein, D. J., & Lange, T. (2014). Safe curves for elliptic-curve cryptography. *Cryptology ePrint Archive*.

Biham, E., Dunkelman, O., & Keller, N. (2006). Related-Key Impossible Differential Attacks on 8-Round AES-192. In D. Pointcheval (Ed.), *Topics in Cryptology – CT-RSA 2006* (pp. 21–33). Springer Berlin Heidelberg.

Chawla, S. S., Aggarwal, S., Kamal, S., & Goel, N. (2015). FPGA implementation of an optimized 8-bit AES architecture: A masked S-Box and pipelined approach. *2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 1–6. https://doi.org/10.1109/CONECCT.2015.7383859

Chen, X. (2020). Implementing AES Encryption on Programmable Switches via Scrambled Lookup Tables. *Proceedings of the Workshop on Secure Programmable Network Infrastructure*, 8–14. https://doi.org/10.1145/3405669.3405819

Daemen, J., & Rijmen, V. (2023). The Design of Rijndael. In *The Design of Rijndael* (1st ed., pp. 53–54). Springer Berlin.

Fan, J., & Verbauwhede, I. (2012). An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost. In D. Naccache (Ed.),

Cryptography and Security: From Theory to Applications: Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday (pp. 265–282). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-28368-0_18

Grassl, M., Langenberg, B., Roetteler, M., & Steinwandt, R. (2015). *Applying Grover's algorithm to AES: Quantum resource estimates* (No. arXiv:1512.04965). arXiv. https://doi.org/10.48550/arXiv.1512.04965

Guha Neogi, P. P. (2022, January). *A Dive into WhatsApp's End-to-End Encryption*. https://doi.org/10.48550/arXiv.2209.11198

Haghighizadeh, F., Attarzadeh, H., & Sharifkhani, M. (2010). A Compact 8-Bit AES Crypto-processor. *2010 Second International Conference on Computer and Network Technology*, 71–75. https://doi.org/10.1109/ICCNT.2010.50

Kautzar, M. G. (2009). Implementasi Sistem Enkripsi Pengirim Pesan Instan Java Dengan Algoritma Blowfish. *Jurnal. Institut Teknologi Bandung. Bandung*.

Kim, H. K., & Sunwoo, M. H. (2019). Low Power AES Using 8-Bit and 32-Bit Datapath Optimization for Small Internet-of-Things (IoT). *Journal of Signal Processing Systems*, *91*(11), 1283–1289. https://doi.org/10.1007/s11265-019-01471-8

Kodali, R. K., & Narasimha Sarma, N. V. S. (2014). Energy Efficient ECC Encryption Using ECDH. In V. Sridhar, H. S. Sheshadri, & M. C. Padma (Eds.), *Emerging Research in Electronics, Computer Science and Technology* (pp. 471–478). Springer India.

Mamun, A., Rahman, S., Shaon, T., & Hossain, Md. A. (2017). Security Analysis of AES and Enhancing its Security by Modifying S-Box with an Additional Byte. *International Journal of Computer Networks & Communications*, *9*, 69–88. https://doi.org/10.5121/ijcnc.2017.9206

Nugroho, A. D., & Munir, R. (2015). Aplikasi Enkripsi Instant Messaging pada Perangkat Mobile dengan menggunakan Algoritma Elliptic Curve Cryptography (ECC). *KNIF*, *2015*, 146–151.

Rabah, K. (2005). Implementation of Elliptic Curve Diffie-Hellman and EC Encryption Schemes. *Information Technology Journal*, *4*(2), 132–139. https://doi.org/10.3923/itj.2005.132.139

Renauld, M., Standaert, F.-X., & Veyrat-Charvillon, N. (2009). Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA. In C. Clavier & K. Gaj (Eds.), *Cryptographic Hardware and Embedded Systems—CHES 2009* (pp. 97–111). Springer Berlin Heidelberg.

Rihan, S. D., Khalid, A., & Osman, S. E. F. (2015). A performance comparison of encryption algorithms AES and DES. *International Journal of Engineering Research & Technology (IJERT)*, *4*(12), 151–154.

Singh, R., Chauhan, A. N. S., & Tewari, H. (2022). Blockchain-enabled End-to-End Encryption for Instant Messaging Applications. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 501–506. https://doi.org/10.1109/WoWMoM54355.2022.00078

Stallings, W. (2002). THE ADVANCED ENCRYPTION STANDARD. *Cryptologia*, *26*(3), 165–188. https://doi.org/10.1080/0161-110291890876

Tsai, K.-L., Huang, Y.-L., Leu, F.-Y., You, I., Huang, Y.-L., & Tsai, C.-H. (2018). AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access*, *6*, 45325–45334. https://doi.org/10.1109/ACCESS.2018.2852563

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Matematika: Jurnal Teori Dan Terapan Matematika*, *15*(1).

Tung, T.-Y., Lin, L., & Lee, D. T. (2012). Pandora Messaging: An Enhanced Self-Message-Destructing Secure Instant Messaging Architecture for

Mobile Devices. *2012 26th International Conference on Advanced Information Networking and Applications Workshops*, 720–725. https://doi.org/10.1109/WAINA.2012.112

Vichare, A., Jose, T., Tiwari, J., & Yadav, U. (2017). Data security using authenticated encryption and decryption algorithm for Android phones. *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 789–794. https://doi.org/10.1109/CCAA.2017.8229903

Vollbrecht, J., Carlson, J. D., Blunk, L., Aboba, Dr. B. D., & Levkowetz, H. (2004). *Extensible Authentication Protocol (EAP)* [RFC 3748]. *3748*. https://doi.org/10.17487/RFC3748

Wen, S., & Dang, W. (2018). Research on Base64 Encoding Algorithm and PHP Implementation. *2018 26th International Conference on Geoinformatics*, 1–5. https://doi.org/10.1109/GEOINFORMATICS.2018.8557068