

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE INTEGRATED ENCRYPTION*
SCHEME PADA PERANGKAT *IOT* UNTUK KEAMANAN DATA *SMART HOME***

Skripsi

Diajukan untuk memenuhi sebagian dari syarat
untuk memperoleh Gelar Sarjana Komputer
Program Studi Ilmu Komputer



Oleh:

Dhafin Kawakibi

1405135

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
BANDUNG
2019**

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE INTEGRATED
ENCRYPTION SCHEME* PADA PERANGKAT *IOT* UNTUK KEAMANAN
DATA *SMART HOME***

Oleh

Dhafin Kawakibi

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

© Dhafin Kawakibi

Universitas Pendidikan Indonesia

2019

Hak Cipta dilindungi undang-undang

skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,
dengan dicetak ulang, difotokopi atau cara lainnya tanpa ijin dari penulis

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE INTEGRATED ENCRYPTION*
SCHEME PADA PERANGKAT *IOT* UNTUK KEAMANAN DATA *SMART HOME***

Oleh

Dhafin Kawakibi

1405135

Disetujui dan Disahkan oleh:

Pembimbing I



Rizky Rahman JP., M.Kom

NIP.197711252006041002

Pembimbing II



Eddy Prasetyo Nugroho, M.T.

NIP. 197505152008011014

Mengetahui,

Ketua Departemen Pendidikan Ilmu Komputer



Lala Septem Riza, M.T., Ph.D.

NIP. 197809262008121001

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE INTEGRATED
ENCRYPTION SCHEME* PADA PERANGKAT *IOT* UNTUK KEAMANAN
DATA *SMART HOME***

Oleh

Dhafin Kawakibi –dhafinkawakibix3@gmail.com

1405135

ABSTRAK

Lingkungan Smart Home dirancang untuk memberi pengguna interaksi minimal pada peralatan rumah tangga seperti kulkas, lampu, pintu, jendela, suhu ruangan dan sebagainya. Sistem Smart Home, terdiri dari beberapa perangkat internet of things (IoT) yang terdiri dari sensor – sensor untuk mengambil data mentah terhadap lingkungan lalu dikirimkan ke server. Namun, komunikasi antara perangkat IoT dengan server dapat dengan mudah diretas oleh pihak luar atau penyerang jika tidak ada langkah pengamanan yang dilakukan. Dalam penelitian ini, kami mengimplementasikan hybrid cryptosystem dengan menggunakan metode keamanan Elliptic Curve Integrated Encryption Scheme (ECIES) yang terdiri dari algoritma Elliptic Curve Cryptography (ECC), AES-128-CBC, pertukaran kunci Diffie-Hellman dan fungsi hash SHA256 untuk mengamankan pesan antara perangkat IoT dan server. Perangkat IoT pada penelitian ini menggunakan NodeMCU dan sensor kelembapan DHT22. Penelitian ini juga menganalisis tingkat randomness pada kunci, aspek privacy pada data dan aspek integrity pada data yang telah di enkripsi dengan metode ECIES. Nilai rata-rata tingkat randomness yang didapatkan dengan menggunakan metode Run Test adalah 0.53644267.

Katakunci—ECIES, elliptic curves, encryption, hybrid cryptosystem, public key cryptography, Smart Home, Internet of things.

**IMPLEMENTASI ALGORITMA *ELLIPTIC CURVE INTEGRATED
ENCRYPTION SCHEME* PADA PERANGKAT *IOT* UNTUK KEAMANAN
DATA *SMART HOME***

Oleh

Dhafin Kawakibi –dhafinkawakibix3@gmail.com

1405135

ABSTRACT

The Smart Home environment was designed to give users minimum interaction with household appliances such as refrigerator, lamp, door, window, room temperature, etc. Smart Home System, consisting of several internet of things (IoT) devices that comprises of sensors to retrieve raw data about the environment followed by sending the data to the server. However, communication between the IoT device and the server can be easily hacked by outsiders or attackers if no security measures were taken. In this study, we implemented a hybrid cryptosystem using the Elliptic Curve Integrated Encryption Scheme (ECIES) security method that consists of Elliptic Curve Cryptography (ECC) algorithm, AES-128-CBC, Diffie-Hellman key exchange and the SHA256 hash function to secure messages between IoT devices and servers. The IoT device in this study used the NodeMCU and the DHT22 humidity sensor. This study also analyzes the level of randomness in keys, privacy aspects of data and integrity aspects of data that had been encrypted with the ECIES method. The average value of the level of randomness obtained using the Run Test method is 0.53644267.

Keywords— ECIES, elliptic curves, encryption, hybrid cryptosystem, public key cryptography, Smart Home, Internet of things.

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	iii
UCAPAN TERIMA KASIH	iv
DAFTAR ISI	vi
DAFTAR GAMBAR	viii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	5
1.3 Tujuan Penelitian	6
1.4 Batasan Masalah	6
1.5 Manfaat Penelitian	6
1.6 Metodologi Penelitian	6
1.6.1 Metodologi Pengumpulan Data	6
1.6.2 Analisis dan Desain Sistem	7
1.6.3 Metode Pembuatan Sistem Enkripsi <i>Smart Home</i>	7
1.7 Sistematika Penulisan.....	7
BAB II TINJAUAN PUSTAKA	9
2.1 <i>Internet of Things</i>	9
2.2 <i>Smart Home</i>	12
2.3 <i>Elliptic Curve Integrated Encryption Scheme (ECIES)</i>	16
2.4 <i>Advanced Encryption Standard (AES)</i>	23
2.5 <i>Secure Hash Algorithm 256 (SHA256)</i>	28
2.6 <i>HTTP Web Service</i>	32
2.7 DHT 22	33
2.8 ESP8266.....	35
BAB III METODE PENELITIAN	37
3.1 Desain Penelitian.....	37
3.1.1. Studi Literatur	38
3.1.2. Analisis dan Desain Sistem	38
3.1.3. Pengembangan Sistem Enkripsi <i>Smart Home</i>	38
3.1.4. Pengujian.....	39
3.1.5. Analisis dan Evaluasi Hasil	40

3.2	Alat dan Bahan Penelitian	41
3.2.1	Alat Penelitian	41
3.2.2	Bahan Penelitian.....	42
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....		43
4.1	Analisis dan Desain Sistem	43
4.2	Pengembangan Sistem Enkripsi <i>Smart Home</i>	44
4.2.1	Perancangan Perangkat IoT	44
4.2.1.1	Pengkodean Perangkat IoT.....	49
4.2.2	Perancangan Web Service <i>Smart Home</i>	50
4.2.2.1	Pengkodean <i>Web Service</i>	51
4.2.3	Perancangan Sistem Enkripsi <i>Smart Home</i>	54
4.2.3.1	Penentuan Algoritma ECC	59
4.2.3.2	Penentuan Algoritma Simetrik	70
4.2.3.3	Penentuan Algoritma <i>Hashing</i>	78
4.2.4	Pengkodean Sistem Enkripsi pada Modul Sensor.....	8
4.2.5	Pengkodean Sistem Dekripsi pada Web Service	11
4.3	Pengujian	15
4.3.1	Pengujian Data Enkripsi.....	15
4.3.2	Pengujian Randomness.....	21
4.4	Analisis dan Evaluasi Hasil.....	23
BAB V KESIMPULAN.....		25
5.1.	Kesimpulan	25
5.2.	Saran	25
DAFTAR PUSTAKA		26

DAFTAR GAMBAR

GAMBAR 1.1 SISTEM <i>SMART HOME</i> (SANTOSO & VUN, 2015).....	2
GAMBAR 2.1 ARSITEKTUR IOT (A: <i>THREE LAYERS</i>) (SETHI & SARANGI, 2017).....	11
GAMBAR 2.2 SKENARIO PENGGUNA (PĂTRU, CARABAŞ, BĂRBULESCU, & GHEORGHE, 2016)	13
GAMBAR 2.3 <i>ELLIPTIC CURVE</i> (DHILLON, 2016)	17
GAMBAR 2.4 PERBANDINGAN ECC DAN RSA DALAM UKURAN KUNCI (DHILLON, 2016).....	18
GAMBAR 2.5 ENKRIPSI DALAM ECIES (V. GAYOSO ET AL., 2010).....	21
GAMBAR 2.7 PROSES ENKRIPSI AES (AKO,2017).....	25
GAMBAR 2.8 S-BOX PADA TIAP BYTE <i>STATE</i> (H. LEE, LEE, & SHIN, 2009).....	25
GAMBAR 2.9 <i>SHIFTRROWS</i> MENGGESER TIGA BARIS PADA <i>STATE</i> (H. LEE ET AL., 2009)	26
GAMBAR 2.10 <i>ADDROUNDKEY</i> (AKO, 2017).....	27
GAMBAR 2.11 <i>CIPHER BLOCK CHAINING (CBC) MODE ENCRYPTION</i> (VAIDEHI & RABI, 2014).....	28
GAMBAR 2.12 DHT 22.....	34
GAMBAR 2.13 ESP8266 (WWW.ESPRESSIF.COM)	35
GAMBAR 2.14 NODEMCU (WWW.NODEMCU.COM)	36
GAMBAR 3.1 DESAIN PENELITIAN.....	37
GAMBAR 4. 1 INFRASTRUKTUR <i>SMART HOME</i>	43
GAMBAR 4.2 ESP12 <i>MODULE</i>	45
GAMBAR 4.3 ESP12 PIN.....	45
GAMBAR 4.4 NODEMCU	47
GAMBAR 4.5 RANGKAIAN MODUL SENSOR SUHU	47
GAMBAR 4.6 BLOK DIAGRAM MODUL SENSOR SUHU	48
GAMBAR 4. 7 SENSOR DHT22	48
GAMBAR 4.8 KODE PEMBACAAN SENSOR DHT22.....	49
GAMBAR 4.9 KODE KONEKSI WIFI	50
GAMBAR 4.10 TERMINAL PERANGKAT IOT	50
GAMBAR 4.11 DIAGRAM <i>WEB SERVICE API RESTFUL</i>	51
GAMBAR 4.12 PENGKODEAN <i>WEB SERVICE</i>	52
GAMBAR 4.13 <i>WEB SERVICE</i> PADA PORT 2500.....	52
GAMBAR 4.14 POST /API/DIFFIEHELLMAN <i>WEB SERVICE</i>	53
GAMBAR 4.15 TAMPILAN TERMINAL <i>WEB SERVICE</i> DIFFIE HELLMAN	53
GAMBAR 4.16 POST /API/ADD-DATA.....	54
GAMBAR 4.17 ENKRIPSI ECIES.....	55
GAMBAR 4.18 DEKRIPSI ECIES.....	56
GAMBAR 4.19 ALUR PROGRAM	57
GAMBAR 4.20 KURVA SECP256K1	61
GAMBAR 4.21 ALUR DIFFIE-HELLMAN ECC	63
GAMBAR 4.22 ALUR AES 128 CBC	71

GAMBAR 4.23 ALUR <i>HASHING SHARED KEY</i>	79
GAMBAR 4.24 ALUR HMAC	79
GAMBAR 4.25 PENGKODEAN MENGHASILKAN KUNCI	92
GAMBAR 4.26 HASIL PENGKODEAN MENGHASILKAN KUNCI	92
GAMBAR 4.27 PENGKODEAN <i>RANDOM NUMBER GENERATOR</i>	93
GAMBAR 4.28 PENGKODEAN <i>SHARED KEY</i>	93
GAMBAR 4.29 HASIL <i>SHARED KEY</i>	93
GAMBAR 4.30 PENGKODEAN ENKRIPSI SIMETRIK.....	94
GAMBAR 4.31 PENGKODEAN <i>HASHING KEY</i>	94
GAMBAR 4.32 PENGKODEAN HMAC.....	95
GAMBAR 4.33 HASIL ENKRIPSI DAN HMAC.....	95
GAMBAR 4.34 FUNGSI DIFFIE-HELLMAN	96
GAMBAR 4.35 FUNGSI DEKRIPSI	97
GAMBAR 4.36 PENGKODEAN PENGIRIMAN DATA DIFFIE HELMAN.....	98
GAMBAR 4.37 HASIL TERMINAL DIFFIE HELLMAN.....	98
GAMBAR 4.38 PENGKODEAN PENGIRIMAN DATA TERENKRIPSI.....	98
GAMBAR 4.39 TERMINAL HASIL PENGIRIMAN DATA ENKRIPSI.....	99
GAMBAR 4.40 SKEMA <i>MAN IN THE MIDDLE</i>	100

DAFTAR TABEL

TABEL 2.1 TABEL FUNGSI KA (V. GAYOSO ET AL., 2010).....	19
TABEL 2.2 TABEL FUNGSI KDF (V. GAYOSO ET AL., 2010).....	19
TABEL 2.3 TABEL FUNGSI ENKRIPSI (V. GAYOSO ET AL., 2010).....	20
TABEL 2.4 TABEL FUNGSI MAC (V. GAYOSO ET AL., 2010).....	20
TABEL 2.5 TABEL FUNGSI HASH (V. GAYOSO ET AL., 2010)	20
TABEL 4.1 HASIL PERBANDINGAN NILAI AKHIR PADA SKENARIO PERTAMA.....	101
TABEL 4.2 TABEL PERBANDINGAN DATA	102
TABEL 4.3 DATA YANG TERSIMPAN PADA DATABASE	103
TABEL 4.4 TABEL HASIL <i>RUN TEST</i>	106

DAFTAR PUSTAKA

- Abdalla, M., Bellare, M., & Rogaway, P. (2001). DHIES: An encryption scheme based on the Diffie-Hellman Problem. *Lecture Notes in Computer Science*, 1–30. https://doi.org/10.1007/3-540-45353-9_12
- Abdalla, M., Bellare, M., & Rogaway, P. (2007). *The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES*. 143–158. https://doi.org/10.1007/3-540-45353-9_12
- Abdallah, A. R., & Shen, X. (2014). Lightweight lattice-based homomorphic privacy-preserving aggregation scheme for home area networks. *2014 6th International Conference on Wireless Communications and Signal Processing, WCSP 2014*. <https://doi.org/10.1109/WCSP.2014.6992067>
- Abomhara, M. (2014). Security and Privacy in the Internet of Things : Current Status and Open Issues. *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference On*, 1–8. <https://doi.org/10.1109/PRISMS.2014.6970594>
- Afreen, R., & Mehrotra, S. C. (2011). a Review on Elliptic Curve Cryptography. *Ijcsit*, 3(3), 84–103.
- Ako, M. A. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. *Cryptography and Network Security*, (June). Retrieved from <https://www.researchgate.net/publication/317615794>
- Ali, W., Dustgeer, G., Awais, M., & Shah, M. A. (2017). *IoT based Smart Home : Security Challenges , Security Requirements and Solutions*. (September), 7–8.
- Al., R. C. et. (2016). *REST APIs: A Large-Scale Analysis of Compliance with Principles and Best Practices. Lecture Notes in Computer Science*,. 9671, 1–18. Retrieved from <https://link.springer.com/content/pdf/10.1007%2F978-3-319-38791-8.pdf>
- Amara, M., & Siad, A. (2011). Elliptic Curve Cryptography and its applications. *7th International Workshop on Systems, Signal Processing and Their Applications (WOSSPA), 2011*, 247–250. <https://doi.org/10.1109/WOSSPA.2011.5931464>
- Aravinthan, V., Namboodiri, V., Sunku, S., & Jewell, W. (2011). Wireless AMI application and security for controlled home area networks. *IEEE Power and Energy Society General Meeting*, 1–8. <https://doi.org/10.1109/PES.2011.6038996>

- Bani Yassein, M., Shatnawi, M. Q., Aljwarneh, S., & Al-Hatmi, R. (2017). *Internet of Things: Survey and open issues of MQTT Protocol*.
- Bellare, M., & Rogaway, P. (2005). *Minimizing the use of random oracles in authenticated encryption schemes*. 1–16. <https://doi.org/10.1007/bfb0028457>
- Berent, A. (2013). Advanced Encryption Standard by Example. Document available at URL <http://www.networkdls.com/Articles/AESbyExample.pdf>
- Bogdan, M. (2016). How to Use the DHT22 Sensor for Measuring Temperature and Humidity with the Arduino Board, *ACTA Universitatis Cibiniensis*, 68(1), 22-25. doi: <https://doi.org/10.1515/aucts-2016-0005>
- Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). *On Privacy and Security Challenges in Smart Connected Homes*. <https://doi.org/10.1109/EISIC.2016.21>
- Burange, A. W., & Misalkar, H. D. (2015). Review of Internet of Things in development of smart cities with data management & privacy. *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015*, 189–195. <https://doi.org/10.1109/ICACEA.2015.7164693>
- Chen, M. (2013). Towards smart city: M2M communications with software agent intelligence. *Multimedia Tools and Applications*, 67(1), 167–178. <https://doi.org/10.1007/s11042-012-1013-4>
- C. Panait and D. Dragomir (2015), “Measuring the performance and energy consumption of aes in wireless sensor networks,” *Proceedings of the Federated Conference on Computer Science and Information Systems*, vol. 5, pp. 1261–1266.
- Dhillon, P. K. (2016). *Elliptic Curve Cryptography for Real Time*. 1–6.
- Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), 469–472. <https://doi.org/10.1109/TIT.1985.1057074>
- Fallis, A. . (2013). For Multi-Gigabyte-Per-Second WPAN and WLAN. *Journal of Chemical Information and Modeling*, 53(9), 1689–1699. <https://doi.org/10.1017/CBO9781107415324.004>

- Gelazanskas, L., & Gamage, K. A. A. (2014). Demand side management in smart grid: A review and proposals for future direction. *Sustainable Cities and Society*, *11*, 22–30. <https://doi.org/10.1016/j.scs.2013.11.001>
- Kalra, S., & Sood, S. (2013). Advanced remote user authentication protocol for multi-server architecture based on ECC. *Journal of Information Security and Applications*, *18*(2–3), 98–107. <https://doi.org/10.1016/j.jisa.2013.07.005>
- Kasgar A. K., Agrawal Jitendra, Sahu Santosh. (2012). “New Modified 256-bit MD5 Algorithm with SHA Compression Function”, *IJCA* (0975–8887) Volume 42 (12) , pp47-51.
- Kiefer, K., Saarlandes, U., & Informatik, G. (n.d.). *A Weakness of the M e n e z e s - V a n s t o n e Cryptosystem*.
- Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*(177), 203–203. <https://doi.org/10.1090/S0025-5718-1987-0866109-5>
- Kocher, P., Lee, R., McGraw, G., & Raghunathan, A. (2004). Security as a new dimension in embedded system design. *DAC '04: Proceedings of the 41st Annual Design Automation Conference*, 753–760. <https://doi.org/10.1145/996566.996771>
- Lee, H., Lee, K., & Shin, Y. (2009). *AES Implementation and Performance Evaluation on 8-bit Microcontrollers*. *6*(1), 70–74. Retrieved from <http://arxiv.org/abs/0911.0482>
- Lee, S., Kim, J., & Shon, T. (2016). User privacy-enhanced security architecture for home area network of Smartgrid. *Multimedia Tools and Applications*, *75*(20), 12749–12764. <https://doi.org/10.1007/s11042-016-3252-2>
- Liao, Y. P., & Hsiao, C. M. (2014). A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. *Ad Hoc Networks*, *18*, 133–146. <https://doi.org/10.1016/j.adhoc.2013.02.004>
- M. Gudgin et al.(2007), “SOAP Version 1.2 Part 1: Messaging Framework (Second Edition),” W3C Recommendation. <http://www.w3.org/TR/soap12-part1/>.
- Mantoro, T., Ayu, M. A., & Binti Mahmud, S. M. (2014). Securing the authentication and message integrity for Smart Home using smart phone. *International Conference on Multimedia Computing and Systems -Proceedings*, *0*, 985–989.

<https://doi.org/10.1109/ICMCS.2014.6911150>

Martínez, V. G., Álvarez, F. H., & Encinas, L. H. (n.d.). *Analysis of ECIES and Other Cryptosystems Based on Elliptic Curves*.

Menezes, A. J., & Vanstone, S. A. (1993). Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, 6(4), 209–224.

<https://doi.org/10.1007/BF00203817>

Muheden, K., Erdem, E., & Vancin, S. (2017). Design and implementation of the mobile fire alarm system using wireless sensor networks. *CINTI 2016 - 17th IEEE International Symposium on Computational Intelligence and Informatics: Proceedings*, 243–246.

<https://doi.org/10.1109/CINTI.2016.7846411>

Neumann, A., Laranjeiro, N., & Bernardino, J. (2018). An Analysis of Public REST Web Service APIs. *IEEE Transactions on Services Computing*, PP(c), 1.

<https://doi.org/10.1109/TSC.2018.2847344>

Pătru, I. I., Carabaş, M., Bărbulescu, M., & Gheorghe, L. (2016). Smart home IoT system. *Networking in Education and Research: RoEduNet International Conference 15th Edition, RoEduNet 2016 - Proceedings*.

<https://doi.org/10.1109/RoEduNet.2016.7753232>

R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. BernersLee. Hypertext Transfer Protocol – HTTP/1.1. Technical Report RFC 2616, The Internet Society, <http://www.ietf.org/rfc/rfc2616.txt>, 1999.

R. Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. Ph.d. dissertation, University of California, Irvine, 2007.

R.T. Fielding (2000), “Architectural Styles and the Design of Network-based Software Architectures,” Ph.D. Thesis, University of California, Irvine

Rahim, S., Javaid, N., Ahmad, A., Khan, S. A., Khan, Z. A., Alrajeh, N., & Qasim, U. (2016). Exploiting heuristic algorithms to efficiently utilize energy management controllers with renewable energy sources. *Energy and Buildings*, 129, 452–470.

<https://doi.org/10.1016/j.enbuild.2016.08.008>

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., ... Vo, S. (2010). 032 A

at statistical test suite for random and pseudorandom number generators for cryptographic applications - special pub. 800-22 - Rev. 1. *NIST Special Publication 800-22, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, (April).*
<https://doi.org/10.6028/NIST.SP.800-22r1a>

Sahu, Aradhana & Ghosh, Samarendra. (2017). Review Paper on Secure Hash Algorithm With Its Variants. 10.13140/RG.2.2.13855.05289.

Santoso, F. K., & Vun, N. C. H. (2015). *Securing IoT for Smart Home System*. 5–6.

Sethi, P., & Sarangi, S. R. (2017). *Internet of Things : Architectures , Protocols , and Applications*. 2017. <https://doi.org/10.1155/2017/9324035>

Siano, P. (2014). Demand response and smart grids - A survey. *Renewable and Sustainable Energy Reviews*, 30, 461–478. <https://doi.org/10.1016/j.rser.2013.10.022>

Standards for Efficient Cryptography SEC 1 : Elliptic Curve Cryptography. (2009). 1(Sec 1).

Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 1–8. <https://doi.org/10.1109/ICSEMR.2014.7043637>

Suresh, S., & Sruthi, P. V. (2016). A review on smart home technology. *IC-GET 2015 - Proceedings of 2015 Online International Conference on Green Engineering and Technologies*, 1–3. <https://doi.org/10.1109/GET.2015.7453832>

V. Gayoso, M., L. Hernández, E., & C. Sánchez, Á. (2010). *Encryption Scheme*. 2(2), 7–13.

Vaidehi, M., & Rabi, B. J. (2014). *Design and Analysis of AES-CBC Mode for High Security Applications*. 499–502.

Workshop, I., & Hutchison, D. (2014). Radio Frequency Identification: Security and Privacy Issues

.W. Diehl, F. Farahmand, P. Yalla, J.-P. Kaps, and K. Gaj (2017). “Comparison of hardware and software implementations of selected lightweight block ciphers,” in 27th International Conference on Field Programmable Logic and Applications (FPL). IEEE pp. 1–4.

Yu, R., & Watteyne, T. (2013). Reliable , Low Power Wireless Sensor Networks for the Internet of Things : Making Wireless Sensors as Accessible as Web Servers. *White Paper WP003*, 1–4.

Z. Shelby (2011), “Embedded Web Services,” lecture slides/
https://noppa.aalto.fi/noppa/kurssi/t-110.5150/luennot/T110_5150_embedded_web_services_in_iot.pdf.