PENERAPAN ALGORITMA *ELLIPTIC CURVE INTEGRATED ENCRYPTION SCHEME (ECIES)* UNTUK KEAMANAN DATA PADA SISTEM *SMART HOME*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat

Memperoleh Gelar Sarjana Komputer

OLEH :

CINDI RAHMA SARI

09011281924151

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2023

HALAMAN PENGESAHAN

PENERAPAN ALGORITMA *ELLIPTIC CURVE INTEGRATED ENCRYPTION SCHEME (ECIES)* UNTUK KEAMANAN DATA PADA SISTEM *SMART HOME*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

CINDI RAHMA SARI
09011281924151

Palembang, 27 Mei 2023

Mengetahui,

Ketua Jurusan Sistem Komputer,	Pembimbing Tugas Akhir,
Dr. Ir. Sukemi, M.T.	**Ahmad Fali Oklilas, M.T.**
NIP. 196612032006041001	**NIP. 197210151999031001**

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Selasa

Tanggal : 11 April 2023

Tim Penguji :

1. **Ketua** : **Dr. Ir. Bambang Tutuko, M.T.**
2. **Sekretaris** : **Abdurrahman, S.Kom., M.Han.**
3. **Penguji** : **Muhammad Ali Buchari, S.Kom., M.T.**
4. **Pembimbing** : **Ahmad Fali Oklilas, M.T.**

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.
NIP. 19661203 200604 1 001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Cindi Rahma Sari

NIM : 09011281924151

Judul : PENERAPAN ALGORITMA *ELLIPTIC CURVE INTEGRATED ENCRYPTION SCHEME (ECIES)* UNTUK KEAMANAN DATA PADA SISTEM *SMART HOME*

Hasil pengecekan *Software Turnitin* : 20%

Menyatakan bahwa Laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam Laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Mei 2023

CINDI RAHMA SARI

HALAMAN PERSEMBAHAN

"Kupersembahkan skripsi ini untuk mama, papa, adik serta keluarga besar ♥"

"Diwajibkan atas kamu berperang, padahal berperang itu adalah sesuatu yang kamu benci. Boleh jadi kamu membenci sesuatu, padahal ia amat baik bagimu, dan boleh jadi (pula) kamu menyukai sesuatu, padahal ia amat buruk bagimu; Allah mengetahui, sedang kamu tidak mengetahui."

(Al-Baqarah Ayat 216)

"Wahai orang-orang yang beriman! Jika kamu menolong (agama) Allah, niscaya Dia akan menolongmu dan meneguhkan kedudukanmu."

(Muhammad Ayat 7)

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahirabbil Alamin, puji dan syukur Penulis panjatkan kepada Allah SWT yang telah melimpahkan nikmat, taufik, dan hidayah-Nya yang sangat besar dan tidak pernah berhenti kepada peneliti sehingga peneliti dapat menyelesaikan Tugas Akhir ini yang berjudul **"Penerapan Algoritma *Elliptic Curve Integrated Encryption Scheme (ECIES)* Untuk Keamanan Data Pada Sistem *Smart Home*"**. Shalawat beriring salam senantiasa tercurahkan kepada Nabi Muhammad Shallallahu Alaihi Wasallam yang telah membawa kedamaian dan rahmat untuk semesta alam serta menjadi suri tauladan bagi umatnya.

Dalam tugas akhir ini peneliti menjelaskan mengenai pengamanan data pada sistem *smart home* dengan menggunakan algoritma *Elliptic Curve Integrated Encryption Scheme* (ECIES). Peneliti berharap agar tulisan ini dapat bermanfaat bagi orang banyak.

Pada kesempatan ini, dengan segala kerendahan hati penulis mengucapkan terima kasih kepada semua pihak atas bantuan, bimbingan, dan saran yang telah diberikan dalam menyelesaikan Tugas Akhir ini, antara lain:

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga saya dapat menyelesaikan Penelitian Tugas Akhir ini dengan baik dan lancar,

2. Orang tua tercinta, Bapak Dedy Cahyono dan Ibu Yoncik, yang telah membesarkan dengan penuh kasih sayang dan selalu mengajarkan dalam berbuat hal yang baik. Terimakasih untuk segala doa, motivasi dan dukungannya,

3. Adik tercinta, Sabila Kurnia Sari, yang selalu memberikan semangat serta dukungannya,

4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan Sistem Komputer di Fakultas Ilmu Komputer Universitas Sriwijaya,

5. Bapak Rahmat Fadli Isnanto, S.Si., M.Sc., selaku Dosen Pembimbing Akademik,

6. Bapak Ahmad Fali Oklilas, M.T., selaku Pembimbing Tugas Akhir yang telah berkenan meluangkan waktunya untuk membimbing, memberikan saran dan motivasi kepada peneliti untuk menyelesaikan Tugas Akhir ini,

7. Ibu Renny Virgasari selaku Admin di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah membantu peneliti dalam hal-hal administrasi,

8. Beasiswa Bidikmisi yang sudah memberikan kesempatan kepada peneliti, untuk bisa menjadi salah satu mahasiswa penerima bantuan dari beasiswa tersebut selama masa perkuliahan,

9. Teman – teman jurusan Sistem Komputer angkatan 2019, khususnya Sahabat peneliti (Wiwik Sagita Aprianti, Rizki Amalia, Lilis Suryan), teman – teman Team TA (Agustinus Yulius Bagus, Sri Nadhila, Anggita Putri Anti, Jumiati, Pitria Putri Sari), dan Sa'ad Abdillah Waqas. Serta semua pihak yang telah membantu baik secara langsung maupun tidak langsung,

10. Seluruh Dosen dan Karyawan Fakultas Ilmu Komputer Universitas Sriwijaya,

11. Almamater,

12. *And the last but not least, I wanna thank me, I wanna thank me for believing in me, I wanna thank me for doing all this hard work, I wanna thank me for having no days off, I wanna thank me for never quitting, for just being me at all times*.

Peneliti menyadari bahwa Tugas Akhir ini masih sangat jauh dari kata sempurna. Untuk itu peneliti sangat terbuka jika ada kritik dan saran yang bersifat membangun agar lebih baik di kemudian hari.

Akhir kata dengan segala keterbatasan, peneliti berharap semoga laporan Tugas Akhir ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbang pikiran dalam peningkatan mutu pembelajaran dan penelitian.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, Mei 2023
Penulis,

CINDI RAHMA SARI
NIM. 09011281924151

Implementation of Elliptic Curve Integrated Encryption Scheme (ECIES) Algorithm for Data Security in Smart Home Systems

Cindi Rahma Sari (09011281924151)

Computer Engineering Department, Computer Science Faculty, Sriwijaya University

Email : rahmacindi7@gmail.com

Abstract

Smart home systems are technologies that continue to evolve. They provide convenience and comfort to users in controlling devices in their homes. However, this convenience poses a high security risk for user data leakage. Therefore, an effective encryption algorithm is needed to secure data in smart home systems. One suitable algorithm for use in smart home systems is the Elliptic Curve Integrated Encryption Scheme (ECIES). This algorithm uses cryptography that is more secure and efficient compared to other algorithms. This study aims to analyze data security in smart home systems and obtain results on how fast this algorithm can perform encryption and decryption. The results show that the average data encryption speed is 0.117 bytes/millisecond and the average data decryption speed is 0.178 bytes/millisecond. The results of this study can be used by smart home application developers to choose the most suitable cryptography algorithm to use in their applications, thereby enhancing user data security and privacy.

Keywords : *Smart home system, Data Security, Elliptic Curve Integrated Encryption Scheme (ECIES), Encryption Speed, Decryption Speed.*

Penerapan Algoritma *Elliptic Curve Integrated Encryption Scheme (ECIES)* Untuk Keamanan Data Pada Sistem *Smart Home*

Cindi Rahma Sari (09011281924151)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : rahmacindi7@gmail.com

Abstrak

Sistem *smart home* merupakan teknologi yang sampai saat ini masih akan terus berkembang. Sistem ini memberikan kemudahan serta kenyamanan bagi penggunanya untuk mengendalikan perangkat – perangkat yang ada di rumah. Akan tetapi, kemudahan ini akan menyebabkan resiko keamanan yang sangat tinggi akan kebocoran data penggunanya. Oleh karena itu diperlukan algoritma enkripsi yang efektif untuk mengamankan data yang ada pada sistem *smart home*. Salah satu algoritma yang cocok digunakan pada sistem *smart home* adalah algoritma *Elliptic Curve Integrated Encryption Scheme* (ECIES). Algoritma ini menggunakan algoritma kriptografi yang lebih aman dan efisien dibandingkan dengan algoritma lainnya. Penilitian ini bertujuan untuk menganalisa keamanan data pada sistem *smart home* serta mendapatkan hasil seberapa cepat algoritma ini melakukan enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa kecepatan rata – rata enkripsi data adalah sebesar 0,117 *bytes/millisecond* dan kecepatan rata – rata dekripsi data adalah sebesar 0,178 *bytes/millisecond*. Hasil penelitian ini nantinya dapat digunakan oleh para pengembang aplikasi *smart home* untuk memilih algoritma kriptografi yang paling cocok untuk digunakan dalam aplikasi mereka, sehingga dapat meningkatkan keamanan dan privasi data pengguna

Kata Kunci : Sistem *smart home*, Keamanan Data, *Elliptic Curve Integrated Encryption Scheme* (ECIES), Kecepatan Enkripsi, Kecepatan Dekripsi.

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR LAMPIRAN

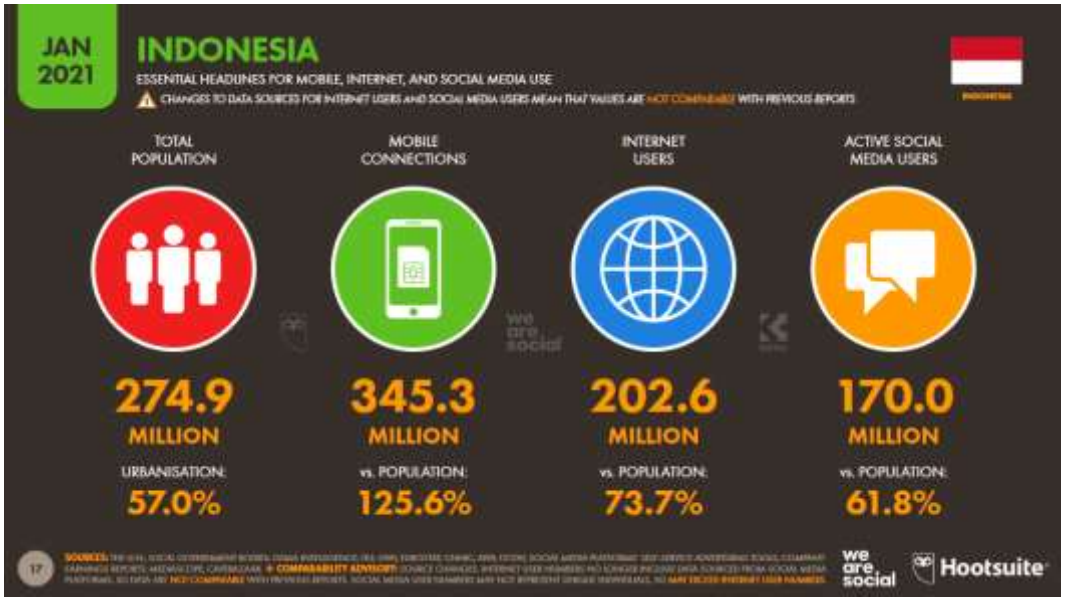
BAB I
PENDAHULUAN

1.1. Latar Belakang

Seiring dengan bertambahnya pengguna internet didunia, penggunaan internet untuk keperluan bisnis, hiburan, dan pendidikan pun semakin berkembang pula. Dengan meningkatnya jumlah pengguna internet didunia, keamanan data yang dimasukkan ke internet pun juga dibutuhkan. Indonesia merupakan salah satu negara yang pertumbuhan jumlah pengguna internetnya masih terus berkembang hingga saat ini.

Menurut Dirjen Aptika Kominfo, Semuel A, dalam webinar VIDA Outlook 2022: Tren Penggunaan Identitas Digital Dalam Mendorong Transformasi Digital Indonesia pada hari Rabu (02/02/2022), pengguna internet di Indonesia sekarang telah mencapai 202,6 juta dan untuk selanjutnya akan selalu bertambah dan akan terus mengalami peningkatan yang sangat signifikan. Jumlah ini meningkat sebanyak 11% dibanding dengan tahun lalu, yakni dari 175,4 juta pengguna [1].

Seperti yang dapat dilihat pada gambar 1.1 yang merupakan data dari Hootsuite, bahwa total masyarakat Indonesia sebanyak 274,9 juta dengan orang yang menggunakan internet sebanyak 202,6 juta atau sebanyak 73,7% dari keseluruhan masyarakat yang ada di Indonesia, dan orang yang menggunakan media sosial secara aktif sebanyak 170 juta atau sebanyak 61,8% dari jumlah penduduk di Indonesia [2]. Adapun menurut [3] penyebab utama dari meningkatnya pertumbuhan pengguna internet di Indonesia adalah berkembangnya infrastruktur serta kemudahan untuk mendapatkan ponsel pintar atau *smartphone*.



Gambar 1.1 Data Tren Pengguna Internet di Indonesia Tahun 2021[2]

Seiring dengan bertambahnya pengguna internet, teknologi informasi pun semakin berkembang pula. Kebutuhan akan perangkat yang bisa mempermudah pekerjaan manusia pun semakin banyak diperlukan. Hal ini membuat peran komputer yang bisa mempermudah pekerjaan manusia pun semakin banyak diperlukan. Adapun komputer yang dibutuhkan adalah komputer yang bisa mengendalikan alat elektronik. Dengan semakin majunya teknologi internet, perangkat elektronik pun dapat dikendalikan dengan internet. Hal ini biasa disebut dengan *Internet of Things* (IoT). *Internet of Things* adalah pengembangan berkelanjutan dari Internet di mana objek elektronik dapat berkomunikasi dan memberikan informasi waktu nyata [4].

Internet of things sendiri adalah konsep yang bertujuan untuk memperluas konektivitas jaringan internet yang tersambung secara terus – menerus. Pada dasarnya intenet of things merupakan sebuah atau banyak benda yang bisa menginterpretasikan sebuah struktur berbasis jaringan internet [5]. Adapun IoT bekerja dengan cara melakukan interaksi antar mesin yang satu dengan mesin yang lainnya yang otomatis terhubung tanpa adanya campur tangan *user* dan dapat dikendalikan dari jarak yang jauh. Internet merupakan penghubung antara mesin satu ke mesin yang lainnya, sementara pengguna hanya bertugas untuk mengatur serta mengawasi cara kerja mesin tersebut [6].

Adapun salah satu produk dari *Internet of Things* yang cukup banyak diketahui oleh masyarakat adalah *Smart home*. *Smart home* adalah penerapan teknologi IoT ke berbagai perangkat di rumah seperti kulkas, lampu, pintu, jendela, suhu ruangan, dan lain lain. *Smart home* adalah teknologi yang dapat menjadikan rumah memiliki sistem otomatis dengan performa yang sangat canggih[7]. Dengan menggunakan teknologi *Smart home* kita bisa mengontrol ataupun mendapat informasi yang dikirim oleh perangkat IoT yang tersambung ke Internet. Internet sendiri sudah menjadi kebutuhn manusia dalam berbagai bidang.

Dengan meningkatnya jumlah pengguna internet menimbulkan masalah baru yaitu kekhawatiran akan keamanan data yang dimasukkan ke intenet[8]. Kekhawatiran ini menjadi perhatian sejak terjadinya beberapa peretasan yang terjadi pada tahun 2021 lalu. Salah satu dari kasus tersebut adalah peretasan situs Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, yaitu bpjs-kesehatan.go.id, yang berujung pada bocornya data milik 279 juta penduduk Indonesia, data ini pada akhirnya dijual di sebuah forum online yang bernama Raid Forums. Adapun data yang telah bocor tersebut dijual dengan harga 0,15 Bitcoin (sekitar Rp. 84.400.000,00, kurs 20 Mei 2021), data – data yang bocor berisi NIK, nomor ponsel, e-mail, alamat, hingga gaji [9]. Hal ini meningkatkan kesadaran masyarakat akan pentingnya mengetahui keamanan data yang dimasukkan ke internet.

Smart Home biasanya membutuhkan perangkat dengan sangat sedikit energi. Oleh karena itu, beberapa *algorithm* tidak cocok digunakan pada *Smart Home*. Salah satu *algorithm* yang menggunakan sedikit energi adalah *Elliptic Curve Cryptography* (ECC)[10]. ECC sendiri merupakan sebuah cryptography algoritm kunci public yang berdasar dengan struktur aljabar dari Eliptic Curve yang ada di daerah finite. ECC diyakini bisa menggantikan cryptography yang berdasar faktorisasi prima atau cryptography daerah finite. Pada saat ini ECC sudah banyak memiliki turunan seperti digital signature (ECDSA, ECPVS), key exchange (ECMQV, ECDH), atapun pada skema enkripsi data (ECIES). ECC menggunakan panjang kunci yang lebih kecil daripada cryptography, meskipun hanya menggunakan panjang kunci yang lebih sedikit daripada algoritma yang

lain, akan tetapi tingkat keamanan yang diperoleh akan sama dengan tingkat keamanan yang diberikan oleh cryptography. Dengan panjang kunci yang lebih kecil, kita bisa mendapatkan beberapa keuntungan yaitu, kecepatan komputasi yang lebih tinggi serta ukuran data yang lebih kecil. Hal ini dapat kita manfaatkan pada sisrtem yang ada di smart home[11].

Eliptic curve integrated encryption scheme (ECIES) adalah salah satu skema yang berdasar pada ECC. ECIES merupakan kombinasi dari assimetric eliptic curve encryption dengan simetric AES serta menggunakan hash SHA-1 algorithm untuk menyediakan encryption scheme yang mendukung enkripsi pesan. ECIES merupakan algoritma yang dirancang secara semantic aman tehadap serangan chosen plaintext attack dan chosen chipertext attack[11]. Algoritma ECIES juag menawarkan rangkaian fitur terbaik sehingga memberikan hasil enkripsi yang aman serta fleksibel [10].

Oleh karena itu, peneliti akan menganalisa keamanan data pada sistem *smart home* dengan mengambil judul "Penerapan Algoritma *Elliptic Curve Integrated Encryption Scheme* (ECIES) Untuk Keamanan Data Pada Sistem *Smart home*".

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan, maka Peneliti merumuskan beberapa masalah dalam penelitian ini, yakni

1. Bagaimana menganalisa keamanan data pada sistem *smart home* dengan menggunakan algoritma *elliptic curve integrated encryption scheme*?
2. Bagaimana kecepatan ekripsi dan dekripsi data menggunakan algoritma *elliptic curve integrated encryption scheme* dalam mengamankan data pada sistem *smart home*?

1.3. Batasan Masalah

Batasan – batasan masalah dalam penulisan Tugas Akhir ini, yaitu :

1. Metode yang digunakan adalah algoritma *elliptic curve integrated encryption scheme* dengan dataset yang digunakan adalah data milik orang lain.
2. Output penelitian ini adalah hanya berupa nilai kecepatan enkripsi dan dekripsi data mengenai pengamanan data pada sistem *smart home* yang dihasilkan dengan algoritma *elliptic curve integrated encryption scheme.*

1.4. Tujuan

Tujuan dari penulisan Tugas Akhir ini, yaitu :

1. Mendapatkan hasil analisa keamanan data pada sistem *smart home* dengan menggunakan algoritma *elliptic curve integrated encryption scheme*.
2. Memberikan gambaran mengenai seberapa cepat algoritma *elliptic curve integrated encryption scheme* dapat mengenkripsi dan mendekripsi data *smart home*.

1.5. Manfaat

Manfaat dari penulisan Tugas Akhir ini, yaitu :

1. Mengetahui keamanan data pada sistem smart home dengan menggunakan algoritma *elliptic curve integrated encryption scheme*.
2. Memberikan pemahaman yang lebih baik tentang kinerja algoritma *elliptic curve integrated encryption scheme* dalam enkripsi dan dekripsi data smart home. Hasil penelitian dapat digunakan oleh para pengembang aplikasi *smart home* untuk memilih algoritma kriptografi yang paling cocok untuk digunakan dalam aplikasi mereka, sehingga dapat meningkatkan keamanan dan privasi data pengguna.

1.6. Sistematika Penulisan Tugas Akhir

Sistematika penulisan tugas akhir ini dibuat untuk mempermudah dan memperjelas isi dalam penyusunan tugas akhir.

1. **PENDAHULUAN**

   Bab ini akan memuat tentang latar belakang dari masalah yang akan diteliti, yang nantinya masalah tersebut akan dirumuskan, kemudian diberi batasan masalah yang akan dibahas, memperjelas tujuan serta manfaat dari penelitian yang dilakukan harapanya dapat memberikan solusi terhadap masalah tersebut.

2. **TINJAUAN PUSTAKA**

   Menjelaskan Beberapa penelitian terkait dan dasar teori yang diperlukan untuk penelitian seperti menjelaskan secara detail metode ataupun algoritma yang akan peneliti gunakan dalam pemecahan masalah dalam penelitian.

3. **METODOLOGI**

   Pembahasan secara rinci mengenai alur proses penelitian dari awal sampai akhir berdasarkan metode yang digunakan.

4. **HASIL DAN PEMBAHASAN**

   Setelah proses penelitian selesai dan didapatkan jawaban dari tujuan yang telah dijelaskan pada bab sebelumnya, selanjutnya peneliti akan melakukan analisa hasil akhir penelitian.

5. **KESIMPULAN DAN SARAN**

   Merujuk pada hasil dan analisa yang telah didapat maka peneliti akan menarik kesimpulan serta memberikan saran untuk penelitian yang akan dilakukan selanjutnya.

DAFTAR PUSTAKA

[1] P. Agustini, “Warganet Meningkat, Indonesia Perlu Tingkatkan Nilai Budaya di Internet,” 2021. [Online]. Available: https://aptika.kominfo.go.id/2021/09/warganet-meningkat-indonesia-perlu-tingkatkan-nilai-budaya-di-internet/.

[2] We Are Social, “Digital 2021,” *Glob. Digit. Insights*, p. 103, 2021.

[3] L. Noviandari, “Hampir setengah penduduk Indonesia mengakses internet pada tahun 2018,” 2018. [Online]. Available: https://id.techinasia.com/jumlah-pengguna-internet-indonesia-2014-2018.

[4] E. Febriana, N. Widiyasono, and ..., “Analisis Keamanan dan Infrastruktur serta Proses Investigasi pada Perangkat Internet of Things (IoT) menggunakan Metode End to End Digital Investigation (EEDI),” *SAIS| Sci. Artic. ...*, vol. 1, no. 2, pp. 137–147, 2018.

[5] Z. D. Dewi Lusita Hidayati Nurul, Rohmah F mimin, “Prototype Smart Home Dengan Modul Nodemcu Esp8266 Berbasis Internet of Things (Iot),” *J. Tek. Inform.*, p. 3, 2019.

[6] E. Oriwoh and M. Conrad, “‘Things’ in the Internet of Things: Towards a Definition,” *Int. J. Internet Things*, vol. 4, no. 1, pp. 1–5, 2015.

[7] E. Sri, R. Achmad, and M. Nurdin, “Perancangan Smart Home Untuk Pengendalian Peralatan Elektronik Dan Pemantauan Keamanan Rumah Berbasis Internet Of Things,” vol. 0266, pp. 119–135.

[8] A. Rizal, “Daftar Kasus Peretasan yang Menghebohkan Indonesia Tahun Ini,” 2021. [Online]. Available: https://infokomputer.grid.id/read/123058110/daftar-kasus-peretasan-yang-menghebohkan-indonesia-tahun-ini.

[9] F. A. Burhan, “Kominfo Tangani 43 Kebocoran Data Tahun Ini, BPJS Kesehatan Belum,” 2021. [Online]. Available: https://katadata.co.id/desysetyowati/digital/61cd8cf0e5173/kominfo-tangani-43-kebocoran-data-tahun-ini-bpjs-kesehatan-belum.

[10] P. Seminar *et al.*, “Implementasi Kriptografi Kurva Eliptik Pada Sistem Keamanan Smart,” no. November, pp. 285–291, 2016.

[11] D. Syahfitra, “Analisis dan Implementasi Elliptic Curve Integrated Encryption Scheme (ECIES).”

[12] E. Balamurugan, M. Sc, and M. Phil, “ELLIPTIC CURVE INTEGRATED ENCRYPTION SECEME USING ANALYSIS VEHICULAR AD HOC NETWORK,” vol. 3, no. 5, pp. 47–50, 2016.

[13] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, “Java card implementation of the elliptic curve integrated encryption scheme using prime and binary finite fields,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6694 LNCS, pp. 160–167, 2011, doi: 10.1007/978-3-642-21323-6_20.

[14] S. Ali and A. Abdul, “Data Security for Cloud Computing based on Elliptic Curve Integrated Encryption Scheme (ECIES) and Modified Identity based Cryptography (MIBC),” *Int. J. Appl. Inf. Syst.*, vol. 10, no. 6, pp. 7–13, 2016, doi: 10.5120/ijais2016451517.

[15] S. Chavhan, “Secured Map Building using Elliptic Curve Cloud-based Robots,” no. Iccmc, pp. 157–164, 2020.

[16] Hossain, M. S., dkk. “An Energy-Efficient and Secure Communication Protocol for Smart Home Systems,” *IEEE Trans. Sustain. Comput.*, vol. 7, no. 1, pp. 59–70, 2022.

[17] Khurana, S. I., dkk. “Securing Smart Home Automation with Elliptic Curve Integrated Encryption Scheme,” *IEEE Internet Things Journal*, vol. 9, no. 1, pp. 555–566, 2022.

[18] Rahim, M., dkk. “Secure smart home communication protocol based on elliptic curve cryptography,” *IEEE Access*, vol. 8, pp. 68204–68215, 2020.

[19] Rahman, M. R., dkk. “Secure and Scalable IoT-Based Smart Home Architecture,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9187–9198, 2020.

[20] Ruparelia, N. N., dkk. “A Robust and Efficient Scheme for Security and Privacy of Smart Home Using Elliptic Curve Cryptography,” *IEEE Sens. J.*, vol. 19, no. 21, pp. 9616–9624, 2019.

[21] R. Mulyawan, “Mengenal Pengertian Smart Home: Fungsi, Manfaat, Karakteristik, Kelebihan dan Kekurangannya,” *May 1st*, 2019.

[22] H. and others Sari, Ika Yusnita and Muttaqin, Muttaqin and Jamaludin, Jamaludin and Simarmata, Janner and Rahman, M Arif and Iskandar, Akbar and Pakpahan, Andrew Fernando and Abdul Karim, Sugianto and Giap, Yo Ceng and Hazriani, “Keamanan Data dan Informasi,” *Yayasan Kita Menulis*, 2020.

[23] Asep, “Apakah Pengertian Akurasi dan Presisi,” 2021. [Online]. Available: https://artikelkeren.com/akurasi-presisi.html#:~:text=Pengertian Akurasi Akurasi mengukur ketepatan dan kemiripan hasil,itu%2C semakin mendekati ukurannya%2C semakin tinggi level akurasi.

[24] Z. Liang, X. Li, H. Zhang, “A high-performance implementation of elliptic curve integrated encryption scheme for wireless sensor networks,” *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 9, pp. 3695–3707, 2020.

[25] A. S. A. Sukor, “Dataset For Smart Home,” 2020. [Online]. Available: https://www.kaggle.com/datasets/shegguy87/dataset-for-smart-home. [Accessed: 21-Jan-2023].