E-ISSN 2460-9552
P-ISSN 2620-3227

MULTI – FACTOR AUTHENTICATION DALAM MENINGKATKAN KEAMANAN PERANGKAT IOT TERHADAP SERANGAN SIBER: *SYSTEMATIC LITERATURE REVIEW*

Hafidh Azizah
Jurusan Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
e-mail: hafidhazizah@gmail.com

Abstract

Security aspects in the development and deployment of IoT devices are often crucial but overlooked. This is evident from the number of IoT devices that are faced with cyber threats due to suboptimal security systems. The reason for this problem is because during the development stage of IoT devices, some developers do not pay special attention to the implementation of strong security protocols. Based on these problems, this literature review aims to examine the extent to which Multi-Factor Authentication (MFA) can improve the security of IoT devices, especially in the face of increasingly complex cyber attacks. This literature review uses the Systematic Literature Review (SLR) method with the PRISMA framework approach to ensure a systematic and analytical review of related literature. Of the 155 journals traced with a time span of 2010 - 2024, 21 journals were obtained that met the predetermined eligibility criteria. Based on the results of the literature review, the implementation of Multi-Factor Authentication (MFA) on Internet of Things (IoT) devices is considered capable of mitigating and handling several security attack threats such as brute force attacks, Man-in-the-Middle (MITM), insider attacks, replay attacks, and other attacks.

Keywords: *Cyber Security; Internet of Things; IoT Security; Multi – Factor Authentication*

Abstrak

Aspek keamanan dalam pengembangan dan penerapan perangkat IoT sering kali menjadi hal yang krusial namun terabaikan. Hal ini terbukti dari banyaknya perangkat IoT yang dihadapkan oleh ancaman siber akibat dari sistem keamanan yang kurang optimal. Penyebab terjadinya permasalahan tersebut karena pada tahap pengembangan perangkat IoT, beberapa *developer* kurang memberikan perhatian khusus terhadap penerapan protokol keamanan yang kuat. Berdasarkan permasalahan tersebut, tinjauan literatur ini memiliki tujuan untuk mengkaji sejauh mana *Multi-Factor Authentication* (MFA) dapat meningkatkan keamanan perangkat IoT, terutama dalam menghadapi serangan siber yang semakin kompleks. Penulisan literatur ini menggunakan metode literatur review yaitu *Systematic Literature Review* (SLR) dengan pendekatan *framework* PRISMA untuk memastikan tinjauan sistematis dan analitis terhadap literatur terkait. Dari 155 jurnal yang ditelusuri dengan rentang waktu 2010 - 2024, diperoleh 21 jurnal yang memenuhi kriteria kelayakan yang telah ditetapkan. Berdasarkan hasil kajian literatur, implementasi *Multi-Factor Authentication* (MFA) pada perangkat *Internet of Things* (IoT) dinilai mampu dalam memitigasi dan menangani beberapa ancaman serangan keamanan seperti serangan *brute force, Man-in-the-Middle* (MITM), *insider attacks*, serangan *replay*, dan serangan lainnya.

Kata Kunci: *Cyber Security; Internet of Things; IoT Security; Multi – Factor Authentication*

1. PENDAHULUAN

Internet of Things (IoT) merupakan salah satu inovasi teknologi yang paling berpengaruh dalam beberapa dekade terakhir [1]. Pesatnya pertumbuhan perangkat IoT tidak lepas dari pengaruh kemajuan teknologi informasi, sensor, dan komputasi yang saling bersinergi dan memungkinkan perangkat untuk terhubung dan berinteraksi secara otomatis [1], [2]. Beberapa manfaat dari integrasi IoT di kehidupan sehari-hari yaitu mengotomatisasi proses, mengumpulkan data secara real-time, serta meningkatkan efisiensi dan efektivitas [3]. IoT telah menjadi satu satu pilar penting dalam transformasi digital yang berkelanjutan karena kemampuannya dalam mempercepat aktivitas dan memberikan solusi yang lebih efisien.

Meskipun IoT menawarkan berbagai manfaat dalam penerapannya, perangkat IoT juga sering kali menghadapi tantangan yang cukup krusial di salah satu aspek yaitu sistem keamanan [4]. Semakin meningkatnya penggunaan perangkat IoT, maka semakin beragam pula ancaman serangan siber yang terjadi [5]. Rentannya sistem keamanan perangkat IoT terhadap serangan siber ini dikarenakan oleh beberapa faktor seperti banyaknya perangkat yang saling terhubung dengan sumber daya yang terbatas, serta pengembang yang kurang memperhatikan detail sistem keamanan selama proses pengembangan perangkat IoT [6]. Para peretas biasanya mengeksploitasi celah keamanan untuk mencuri data ataupun mengambil alih kontrol [4], [6]. Untuk mengatasinya diperlukan sebuah pendekatan keamanan yang bisa memberikan implikasi positif terhadap IoT sehingga dapat melindungi data dan mencegah potensi risiko yang dapat mengganggu fungsionalitas teknologi.

Salah satu pendekatan yang digunakan untuk mengatasi masalah keamanan IoT adalah dengan menggunakan *multi factor authentication* [7]. Pendekatan keamanan ini memungkinkan pengguna untuk menggunakan lebih dari satu metode verifikasi identitas pengguna seperti halnya menggunakan kombinasi antara kata sandi, token dan biometrik [8]. Pendekatan MFA dapat memperkuat sistem keamanan karena menggunakan lapisan perlindungan yang ekstra sehingga mengurangi risiko akses ilegal, dan meningkatkan kepercayaan terhadap perangkat IoT [8], [9].

Dalam pengembangan dan penerapan perangkat IoT**,** aspek keamanan sering kali menjadi hal yang krusial namun terabaikan. Hal ini terbukti dari banyaknya perangkat IoT yang dihadapkan oleh ancaman siber akibat dari sistem keamanan yang kurang optimal. Penyebab terjadinya permasalahan tersebut karena pada tahap pengembangan perangkat IoT, beberapa *developer* kurang memberikan perhatian khusus terhadap penerapan protokol keamanan yang kuat [7]. Akibatnya, perangkat IoT menjadi lebih rentan terhadap serangan siber, seperti pencurian data, pengambilalihan perangkat, atau penyalahgunaan. Berdasarkan permasalahan tersebut, tinjauan literature ini memiliki tujuan yaitu untuk mengkaji sejauh mana *multi factor authentication* dapat meningkatkan keamanan perangkat IoT terutama dalam menghadapi serangan siber yang semakin kompleks.

2. METODE

Penulisan literatur ini menggunakan salah satu metode literatur *review* yaitu *Systematic Literature Review* (SLR) dengan pendekatan *framework* PRISMA yang bertujuan membantu dalam melakukan tinjauan sistematis dan analitis terhadap literatur yang relevan dengan topik penelitian. Adapun dalam melakukan penulisan literatur ini, penulis melakukan beberapa tahapan penulisan untuk menunjang kelengkapan dari paper ini. Tahapan – tahapan yang dilakukan dalam studi literatur ini antara lain: 1) menentukan *research question*; 2) menelusuri dan mengumpulkan literatur yang relevan; 3) menentukan kriteria kelayakan; 4) melakukan skrining literatur yang dikumpulkan; dan 5) menganalisis hasil dan pembahasan.

2.1 *Research Question*

Penulisan ini bertujuan melakukan *Systematic Literature Review* (SLR) untuk mengkaji sejauh mana MFA dapat meningkatkan keamanan perangkat IoT terutama dalam menghadapi serangan siber yang semakin kompleks. Oleh karena itu penulis mengidentifikasi beberapa pertanyaan terkait yang ingin dijawab di dalam paper ini.

RQ1: Bagaimana penerapan *multi factor authentication* (MFA) pada perangkat IoT mampu mengatasi berbagai jenis serangan siber?

RQ2: Jenis serangan siber apa yang dapat ditangani oleh *multi factor authentication*?

RQ3: Apa saja tantangan yang dihadapi dalam penerapan MFA pada perangkat IoT, dan bagaimana hal ini berdampak pada tingkat keamanan?

RQ4: Seberapa efektifkah MFA dalam mengurangi risiko serangan siber pada perangkat IoT dibandingkan dengan metode autentikasi tradisional?

2.2 Pencarian Literatur

Pada tahap ini, penulis melakukan pencarian dan mengumpulkan jurnal-jurnal yang relevan dengan topik penelitian. Untuk menunjang proses tinjauan dan pencarian literatur, penulis menggunakan alat bantu berupa *Publish or Perish, Mendeley, SciHub, Google Translate, typeset.io*, dan *Google Sheet*. Selama proses pencarian literatur, penulis menggunakan *tools Publish or Perish* untuk mengidentifikasi jurnal yang terindeks *Scopus* pada rentang waktu 2010 – 2024 dengan menggunakan kata kunci yaitu *cyber*

E-ISSN 2460-9552
P-ISSN 2620-3227

security, internet of things, IoT security, dan *multi–factor authentication*. Kemudian untuk proses pengumpulan jurnal penulis menggunakan alat bantu *Mendeley* dan *SciHub* untuk memudahkan pengelolaannya. *Mendeley* berfungsi dalam pengelolaan referensi jurnal, sedangkan *SciHub* digunakan untuk mengunduh jurnal yang aksesnya tidak terbuka. Untuk menunjang proses tinjauan literatur, penulis juga menggunakan *typeset.io* sebagai alat untuk mereview isi dari jurnal, *Google Translate* sebagai penerjemah, dan terakhir *Google Sheet* untuk mengatur isi jurnal yang diperlukan selama proses tinjauan.

2.3 Kriteria Inklusi dan Eksklusi

Dalam menentukan literatur yang relevan dan sesuai dengan topik penelitian yang akan dibahas, penulis menentukan beberapa kriteria kelayakan yang terdiri dari kriteria inklusi dan eksklusi.

Tabel 1 Kriteria Kelayakan

Kriteria Inklusi	● Literatur diperoleh dari jurnal yang terindeks *Scopus*. ● Literatur diterbitkan dalam rentang waktu 2010 – 2024. ● Literatur baik secara langsung maupun tidak langsung menjawab satu atau lebih *research question.*
Kriteria Eksklusi	● Literatur yang tidak relevan dan tidak berhubungan dengan topik penelitian. ● Literatur yang hanya tersedia berupa abstraknya saja, tidak tersedia teks lengkapnya.

2.4 Skrining Literatur

Jurnal atau literatur yang telah dikumpulkan sebelumnya akan disaring berdasarkan kriteria kelayakan yang telah ditentukan. Berdasarkan hasil pencarian dengan menggunakan kata kunci *cyber security, internet of things, IoT security*, dan *multi–factor authentication d*an dalam rentang waktu 2010 – 2024 diperoleh 155 jurnal terkait yang terindeks *Scopus*. Selanjutnya dari 155 jurnal tersebut, penulis melakukan penyaringan berdasarkan kriteria inklusi dan eksklusi, sehingga terdapat 21 jurnal terkait yang akan digunakan selama proses tinjauan literatur ini.

3. HASIL DAN PEMBAHASAN

3.1 Penerapan MFA pada Perangkat IoT dalam Mengatasi Serangan Siber

Tabel 1 Implementasi MFA

Ref	Implementasi MFA	Deskripsi
[10], [11], [12], [13], [14], [15]	Autentikasi Dua Faktor (2FA)	Mengharuskan pengguna untuk memberikan dua bentuk identifikasi berbeda seperti kombinasi kata sandi dan PIN yang kompleks untuk mendapatkan akses penggunaan perangkat IoT.
[10], [11], [16], [17], [18], [19], [20], [21]	Autentikasi Biometrik	Mengharuskan pengguna untuk memberikan bentuk identifikasi permanen berupa sidik jari ataupun pengenalan wajah. Misalnya dengan memanfaatkan teknologi ekstraktor fuzzy.
[10]	Enkripsi Ujung ke Ujung (E2EE)	Metode mengenkripsi data yang ditransmisikan antara perangkat IoT dengan *cloud*.
[10]	Algoritma Hash	Penggunaan algoritma hash yaitu SHA-256 digunakan untuk mengamankan data dengan memadatkan data agar lebih rumit untuk di deskripsi.
[11], [22]	Autentikasi Berbasis Atribut	Bentuk autentikasi yang berfokus pada verifikasi identitas perangkat IoT berdasarkan atribut tertentu.

[23]	Protokol Autentikasi	Bagian dari strategi autentikasi yang menekankan verifikasi formal untuk keamanan perangkat IoT, meliputi RADIUS, CoAP, TACACS, TACACS+, dan Kerberos.
[24]	Autentikasi Berbasis Sensor Oportunistik	Memanfaatkan data dari sensor perangkat IoT seperti input audio dan visual untuk membuat faktor autentikasi tambahan sehingga sistem dapat meningkatkan ketahanan mekanisme autentikasi.
[12]	Akselerometer dengan Deteksi Ketukan	Memungkinkan perangkat untuk mengenali interaksi fisik seperti ketukan yang unik sebagai bentuk autentikasi. Biasanya cocok untuk lingkungan dimana perangkat mungkin rentan terhadap serangan spoofing, seperti MAC, IP, dan *spoofing* tag VLAN.
[17], [21]	Integrasi Kartu Pintar	Token fisik yang harus dimiliki pengguna untuk mengautentikasi identitas misalnya kartu pintar.
[15], [17], [25]	Manajemen Kunci Dinamis	Melibatkan penggunaan kunci khusus sesi yang sering berubah, sehingga menyulitkan penyerang dalam mengeksploitasi kredensial yang dicuri.
[18]	Perangkat Seluler Cerdas	Memanfaatkan integrasi perangkat seluler sebagai bentuk autentikasi sehingga memungkinkan verifikasi identitas yang lebih fleksibel dan aman.
[25]	Model Tantangan-Respon	Proses autentikasi yang menggunakan model tanggapan-tantangan di mana server akan memberikan tantangan baru kepada perangkat IoT untuk memverifikasi kredensial identitas.
[19]	Teknik Pemisahan Rahasia	Melibatkan pendekatan pemisahan rahasia yaitu dengan membagu template biometrik menjadi dua bagian yaitu satu bagian untuk di server dan bagian lainnya untuk kartu pintar.
[19]	Enkripsi dan Pertukaran Kunci	Sistem IoT menggunakan algoritma enkripsi dan pertukaran kunci seperti Diffie-Hellman untuk berbagi kunci melalui jaringan secara aman.
[26]	Skema Autentikasi Bertingkat	Melibatkan autentikasi tiga tingkat yang dikelola oleh *Trusted Authority* (TA) meliputi tingkat pertama (verifikasi minimal) yang memungkinkan pengguna membaca file yang disimpan di *cloud* publik; tingkat kedua (verifikasi lebih tinggi) yang memungkinkan pengguna untuk mengunduh file di cloud publik; dan

E-ISSN 2460-9552
P-ISSN 2620-3227

		tingkat ketiga (verifikasi ketat) untuk memastikan hanya pengguna yang berwenang yang dapat mengakses data *sensitive*.
[27]	*Radio Frequency Fingerprinting* (RFF)	Teknik autentikasi yang memanfaatkan karakteristik unik dari sinyal radio yang dipancarkan perangkat IoT untuk memverifikasi identitas.
[21]	Kriptografi Kurva Elliptic (ECC)	Memberikan keamanan tingkat tinggi dibandingkan dengan kriptografi kunci publik tradisional karena mengimplementasikan ukuran kunci yang lebih kecil dan mengarah pada perhitungan yang lebih cepat.

3.2 Serangan yang Dapat Ditangani MFA

Dalam studi [17] menyebutkan beberapa jenis serangan spesifik yang mampu ditangani oleh MFA seperti serangan *brute force, Smart Card Loss Attack* (SCLA), *Session Specific Temporary Information Attack* (SSTIA), serangan peniruan personalisasi, dan serangan yang berasal dari penyalahgunaan hak akses individu (*Insider Attacks*).

Penelitian [13] mengidentifikasi jenis serangan yang dapat dimitigasi oleh metode autentikasi yaitu serangan *spyware,* serangan rekayasa social, *dictionary attack*, serangan berselancar bahu, serangan *brute force,* dan serangan *lexicon.* Sedangkan dalam literatur [18] menunjukan beberapa serangan yang dapat ditahan oleh protokol autentikasi MFA diantaranya serangan penyadapan, serangan lalu lintas (*Distributed Denial of Service*), serangan *replay*, serangan *Man-in-the-Middle* (MITM), serangan *insider attacks,* dan *dictionary attack*.

Studi [25] menguraikan beberapa serangan yang dapat dimitigasi oleh model MFA yaitu serangan *replay*, serangan *Man-in-the-Middle* (MITM), serangan *spoofing* lokasi, dan serangan curian kunci. Sementara menurut penelitian [19], beberapa serangan yang dapat ditangani oleh MFA secara efektif adalah serangan faktor autentikasi, serangan *Man-in-the-Middle, dictionary attack, insider attacks,* dan serangan jaringan.

Pada penelitian [28] mengidentifikasi beberapa ancaman serangan yang dapat dimitigasi oleh protokol autentikasi yaitu serangan *replay,* serangan pemalsuan identitas, kebocoran privasi, serangan *Denial of Service* (DoS), dan *brute force attacks.* Studi [26] menyebutkan beberapa ancaman yang dapat dimitigasi oleh implementasi MFA yaitu serangan terhadap akses tidak sah, pelanggaran data, serangan *phishing,* dan serangan *Man-in-the-Middle* (MITM).

Berdasarkan penelitian [27], implementasi MFA dalam konteks keamanan perangkat IoT dapat mengatasi ancaman serangan berupa serangan *Man-in-the-Middle* (MITM), serangan peniruan personalisasi, serangan *replay,* serangan *jamming,* dan serangan akses tidak sah. Pada penelitian [21], skema autentikasi berbasis ECC secara efektif dapat menolak beberapa serangan seperti serangan *replay,* serangan *Man-in-the-Middle* (MITM), serangan integritas, serangan terhadap pencurian kunci pintar, dan *insider attacks.*

3.3 Tantangan Penerapan MFA pada Perangkat IoT

Penerapan *Multi Factor Authentication* (MFA) pada perangkat IoT menghadirkan beberapa tantangan yang nantinya akan berdampak pada tingkat keamanan secara keseluruhan. Beberapa tantangan dalam penerapan MFA pada perangkat IoT antara lain:

a. Menyeimbangkan kenyamanan pengguna dengan keamanan. Penerapan MFA sering membutuhkan proses yang rumit sehingga menyebabkan beberapa pengguna menolak untuk mengadopsi langkah-langkah keamanan tersebut, hal ini menyebabkan pengguna lebih memilih praktik keamanan yang sederhana dibandingkan dengan yang rumit [10], [12], [13], [17], [18], [19], [24], [29], [30].

b. Keterbatasan sumber daya, banyak perangkat IoT memiliki daya komputasi, masa pakai baterai, dan memori yang terbatas. Oleh karena itu, sulit dalam menerapkan MFA yang kompleks dan menghambat kemampuan dalam proses pemeriksaan autentikasi [10], [11], [12], [13], [17], [18], [19], [24], [27].
c. Risiko keamanan akses, kurangnya mekanisme autentikasi yang kuat misalnya kerentanan autentikasi biometrik. Data biometrik dapat dipalsukan atau direplikasi sehingga berisiko menyebabkan akses tidak sah ke jaringan IoT [10], [18], [24], [27].
d. MFA sering bergantung pada konektivitas jaringan untuk mengirim kode verifikasi atau pemberitahuan [10].
e. Kompleksitas integrasi MFA ke dalan sistem IoT. Meskipun integrasi dapat meningkatkan keamanan perangkat IoT seperti kombinasi mekanisme autentikasi, namun perlu dipertimbangkan bagaimana cara berbagai faktor untuk saling berinteraksi dan potensi risiko apa yang timbul dari kombinasi tersebut [10], [12], [13], [17], [18], [24].
f. Keberagaman lingkungan IoT dapat menyebabkan sulitnya standarisasi protokol MFA sehingga sulit dalam menerapkan langkah-langkah keamanan yang konsisten [12], [24], [27].
g. Kurangnya standardisasi MFA di lingkungan IoT sehingga menciptakan kerentanan keamanan, hal ini disebabkan oleh cara penerapan MFA yang berbeda di masing-masing produsen perangkat IoT [17], [27].
h. Meningkatkan potensi serangan, karena setiap faktor autentikasi tambahan akan memperkenalkan potensi kerentanan baru yang dapat di eksploitasi oleh penyerang [13], [17], [18].
i. Biaya implementasi yang mahal, melibatkan teknik seperti kriptografi atau token perangkat keras yang relatif memerlukan biaya yang banyak akan menyebabkan organisasi mungkin ragu dalam berinvestasi terutama untuk penerapan IoT skala besar [13], [18].
j. Masalah privasi pengguna, integrasi MFA terutama autentikasi biometrik akan menimbulkan keresahan pengguna dalam membagikan informasi biometrik mereka karena takut akan penyalahgunaan dan pelanggaran data [19].
k. Akurasi metode autentikasi, banyak sistem yang masih berusaha dalam mempertahankan akurasi yang tinggi di luar kondisi idealnya [27].

3.4 MFA VS Metode Autentikasi Tradisional

Tabel 2 MFA VS Metode Autentikasi Tradisional

Ref	MFA	Metode Autentikasi Tradisional
[10], [11], [12], [13], [16], [17], [19], [23], [24], [30]	Membutuhkan beberapa lapisan verifikasi sehingga sulit bagi penyerang untuk mendapatkan akses.	Hanya menggunakan satu kata sandi sehingga lebih rentan terhadap serangan siber.
[10], [11], [16], [17]	Memberikan peringatan kepada pengguna jika terjadi akses tidak sah.	Tidak memberikan peringatan hingga pengguna tidak menyadari adanya pelanggaran.
[10], [11]	Integrasi enkripsi data seperti SHA-256 untuk mengamankan data serta mengurangi risiko pencurian data.	Tidak menyertakan enkripsi kuat seperti enkripsi data, sehingga rentan terhadap serangan *phishing.*
[16]	Integrasi keamanan biometrik memberikan tingkat verifikasi yang lebih tinggi.	Hanya mengandalkan faktor berbasis pengetahuan, seperti kata sandi.
[17], [19], [21], [25]	MFA efektif dalam memitigasi dan melawan ancaman serangan karena membutuhkan lebih dari kata sandi.	Metode tradisional lebih rentan terhadap ancaman serangan seperti serangan *brute force, phishing,* dan sebagainya.
[17], [25]	Menyertakan penggunaan manajemen	Menggunakan manajemen kunci statis.

E-ISSN 2460-9552
P-ISSN 2620-3227

	kunci yang dinamis.	
[13]	Penggunaan teknik kriptografi seperti nilai *nonce* dan kode autentikasi pesan (MAC), hal ini dapat meningkatkan keamanan data yang dipertukarkan antar perangkat IoT.	Tidak menggunakan mekanisme yang kuat seperti teknik kriptografi.
[25]	MFA menggabungkan verifikasi konteks yang menilai legitimasi lingkungan operasional perangkat IoT.	Tidak mempertimbangkan faktor kontekstual sehingga rentan terhadap serangan seperti serangan *spoofing* lokasi.
[25]	Menggunakan metode dua arah yaitu tanggapan-tantangan yang mengharuskan server dan perangkat IoT untuk saling mengautentikasi.	Hanya menggunakan metode satu arah.
[21]	MFA dapat dirancang agar mampu mengakomodasi banyak perangkat IoT tanpa mengorbankan keamanan.	Metode tradisional sulit dalam melakukan skalabilitas seiring dengan bertambahnya jumlah perangkat IoT.

3.5 Diskusi

Penerapan MFA secara signifikan dapat meningkatkan keamanan perangkat IoT terhadap ancaman serangan siber seperti serangan *brute force, Man-in-the-Middle* (MITM), *insider attacks*, maupun serangan *replay*. Berbagai model keamanan MFA, seperti autentikasi biometrik dan kriptografi kurva eliptik, dinilai efektif dalam melindungi perangkat IoT dari akses tidak sah dengan cara menambahkan lapisan keamanan. Meskipun penerapan MFA masih menghadapi sejumlah tantangan, namun tingkat efektivitas proteksi serangannya jauh lebih tinggi dibandingkan dengan metode autentikasi tradisional. Fokus dari studi [7] berkaitan dengan protokol dan aplikasi IoT tanpa mengidentifikasi efektivitas penerapan MFA pada perangkat IoT. Hal ini menunjukan kesenjangan yang diisi oleh paper ini, yang mengkaji secara sistematis penerapan MFA dalam konteks keamanan perangkat IoT. Hasil tinjauan literatur menunjukan bahwa MFA dikenal efektif dalam mengatasi serangan siber tertentu, namun apabila penerapannya tidak tepat atau kurang dalam standarisasi, maka dapat menyebabkan kerentanan baru.

4. KESIMPULAN

Berdasarkan hasil kajian literatur, implementasi *Multi-Factor Authentication* (MFA) pada perangkat *Internet of Things* (IoT) dinilai mampu dalam memitigasi dan menangani beberapa ancaman serangan keamanan. Model implementasi MFA seperti autentikasi biometrik, autentikasi dua faktor, *Radio Frequency Fingerprinting* (RFF), dan Kriptografi Kurva Elliptic (ECC) terbukti mampu mencegah dan melindungi perangkat IoT dari beberapa serangan siber seperti serangan *brute force, Man-in-the-Middle* (MITM), *insider attacks,* serangan *replay*, dan serangan lainnya. Dengan menggunakan lebih dari satu lapisan faktor autentikasi, sistem keamanan perangkat IoT akan menjadi lebih kuat dan penyerang akan kesulitan dalam menembus sistem keamanan karena harus melewati beberapa lapisan keamanan. Namun, penerapan MFA sendiri masih menghadapi sejumlah tantangan yang cukup berpengaruh terhadap tingkat keamanan perangkat IoT, hal ini dapat diidentifikasi dari terbatasnya sumber daya, sulitnya menyeimbangkan kenyamanan pengguna dengan keamanan, kompleksitas integrasi MFA, kurangnya standarisasi penerapan MFA di lingkungan IoT, dan lain sebagainya. Menilik dari beberapa tantangan implementasi MFA, hal tersebut tidak mempengaruhi tingkat efektivitas yang ditawarkan oleh MFA dalam mengurangi risiko serangan keamanan perangkat IoT. Dibandingkan dengan metode autentikasi tradisional yang jauh lebih rentan terhadap serangan siber, MFA dinilai lebih efektif dalam mengatasi dan mengurangi tingkat serangan siber pada perangkat IoT. Oleh karena itu, kajian

literatur selanjutnya dapat lebih berfokus pada metode keamanan perangkat IoT yang berbeda serta mampu mengatasi serangan siber dengan tingkat kesulitan yang lebih tinggi.

5. REFERENSI

[1] M. Wu and X. Chen, "Application of Internet of Things and embedded technology in electronic communication," *Meas. Sens.*, vol. 34, p. 101246, Aug. 2024, doi: 10.1016/j.measen.2024.101246.

[2] C. Fernandez-Gago, D. Ferraris, R. Roman, and J. Lopez, "Trust interoperability in the Internet of Things," *Internet Things*, vol. 26, p. 101226, Jul. 2024, doi: 10.1016/j.iot.2024.101226.

[3] Z. Xie, W. Bu, H. Feng, and Y. Wang, "Integrated development of the industrial chain and innovation chain of high-tech manufacturing industry based on the Internet of Things," *Alex. Eng. J.*, vol. 108, pp. 828–838, Dec. 2024, doi: 10.1016/j.aej.2024.09.052.

[4] S. F. Ahmed, Md. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," *Inf. Fusion*, vol. 102, p. 102060, Feb. 2024, doi: 10.1016/j.inffus.2023.102060.

[5] V. Padmavathi and R. Saminathan, "Chapter 19 - Security for the Internet of Things," in *Computer and Information Security Handbook (Fourth Edition)*, J. R. Vacca, Ed., Morgan Kaufmann, 2025, pp. 353–368. doi: 10.1016/B978-0-443-13223-0.00019-9.

[6] Zaed Mahdi, Nada Abdalhussien, Naba Mahmood, and Rana Zaki, "Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms," *Comput. Mater. Contin.*, vol. 80, no. 2, pp. 2139–2159, Aug. 2024, doi: 10.32604/cmc.2024.053542.

[7] Dr. S. Choudhary and G. Meena, "Internet of Things: Protocols, Applications and Security Issues," *Procedia Comput. Sci.*, vol. 215, pp. 274–288, Jan. 2022, doi: 10.1016/j.procs.2022.12.030.

[8] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things Security–A review," *Cyber Secur. Appl.*, vol. 3, p. 100057, Dec. 2025, doi: 10.1016/j.csa.2024.100057.

[9] "Internet of Things Authentication Protocols: Comparative Study," *Comput. Mater. Contin.*, vol. 79, no. 1, pp. 65–91, Apr. 2024, doi: 10.32604/cmc.2024.047625.

[10] R. Kanmani, "Secure communication using light-weight cryptography and 2-factor verification for Iot devices," *Pak. J. Biotechnol.*, vol. 14, no. 3, pp. 459–462, 2017.

[11] K. Y. Lam, "Identity in the internet-of-things (IoT): New challenges and opportunities," *Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.*, vol. 9977, no. Query date: 2024-09-24 19:15:48, pp. 18–26, 2016, doi: 10.1007/978-3-319-50011-9_2.

[12] S. Rajashree, "Security Model for Internet of Things End Devices," *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things Green Comput. Commun. Cyber Phys. Soc. Comput. Smart Data Blockchain Comput. Inf. Technol. IThingsGreenComCPSComSmartDataBlockchainCIT 2018*, no. Query date: 2024-09-24 19:15:48, pp. 219–221, 2018, doi: 10.1109/Cybermatics_2018.2018.00066.

[13] M. K. Rao, "Multi factor user authentication mechanism using internet of things," *ACM Int. Conf. Proceeding Ser.*, no. Query date: 2024-09-24 19:16:25, 2019, doi: 10.1145/3339311.3339335.

[14] P. Jain, "MAFIA: Multi-layered Architecture for IoT-based Authentication," *Proc. - 2020 2nd IEEE Int. Conf. Trust Priv. Secur. Intell. Syst. Appl. TPS-ISA 2020*, no. Query date: 2024-09-24 19:16:25, pp. 199–208, 2020, doi: 10.1109/TPS-ISA50397.2020.00035.

[15] M. Safkhani, "RESEAP: An ECC-Based Authentication and Key Agreement Scheme for IoT Applications," *IEEE Access*, vol. 8, no. Query date: 2024-09-24 19:16:25, pp. 200851–200862, 2020, doi: 10.1109/ACCESS.2020.3034447.

[16] R. F. Al-Mutawa, "A smart home system based on internet of things," *Int. J. Adv. Comput. Sci. Appl.*, no. 2, pp. 260–267, 2020, doi: 10.14569/ijacsa.2020.0110234.

[17] M. Gowtham, "Secure Internet-of- Things: Assessing Challenges and Scopes for NextGen Communication," *2019 2nd Int. Conf. Intell. Comput. Instrum. Control Technol. ICICICT 2019*, no. Query date: 2024-09-24 19:15:48, pp. 151–158, 2019, doi: 10.1109/ICICICT46008.2019.8993327.

[18] A. J. Mohammed, "Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device," *Cryptography*, vol. 3, no. 3, pp. 1–222, 2019, doi: 10.3390/cryptography3030024.

[19] R. Shah, "A multifactor authentication system using secret splitting in the perspective of Cloud of Things," *2017 Int. Conf. Emerg. Trends Innov. ICT ICEI 2017*, no. Query date: 2024-09-24 19:16:25, pp. 1–4, 2017, doi: 10.1109/ETIICT.2017.7977000.

[20] M. Najam-Ul-Islam, "Recursive Cryptanalysis of the IoT Authentication Protocol," *Proc. - 2019 IEEE 1st Glob. Power Energy Commun. Conf. GPECOM 2019*, no. Query date: 2024-09-24 19:16:25, pp. 1–4, 2019, doi: 10.1109/GPECOM.2019.8778569.

[21] P. Dhillon, "A secure multi-factor ECC based authentication scheme for Cloud-IoT based healthcare services," *J. Ambient Intell. Smart Environ.*, vol. 11, no. 2, pp. 149–164, 2019, doi: 10.3233/AIS-190516.

[22] D. Shehada, "Performance Evaluation of a Lightweight IoT Authentication Protocol," *2020 3rd Int. Conf. Signal Process. Inf. Secur. ICSPIS 2020*, no. Query date: 2024-09-24 19:16:25, 2020, doi: 10.1109/ICSPIS51252.2020.9340146.

[23] H. Rekha, "Model Checking M2M and Centralised IOT authentication Protocols," *J. Phys. Conf. Ser.*, vol. 2161, no. 1, 2022, doi: 10.1088/1742-6596/2161/1/012042.

[24] M. Saideh, "Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things," *Sensors*, vol. 24, no. 14, 2024, doi: 10.3390/s24144621.

[25] M. Mehta, "EFFICIENT FRAMEWORK OF SECURITY FOR INTERNET OF THINGS," *Reliab. Theory Appl.*, vol. 19, no. 1, pp. 217–227, 2024, doi: 10.24412/1932-2321-2024-177-217-227.

[26] S. Atiewi, "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," *IEEE Access*, vol. 8, no. Query date: 2024-09-24 19:16:25, pp. 113498–113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

[27] A. Haenel, "Practical cross-layer radio frequency-based authentication scheme for internet of things," *Sensors*, vol. 21, no. 12, 2021, doi: 10.3390/s21124034.

[28] K. Fan, "Lightweight NFC protocol for privacy protection in mobile IoT," *Appl. Sci. Switz.*, vol. 8, no. 12, 2018, doi: 10.3390/app8122506.

[29] B. Chatterjee, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, 2019, doi: 10.1109/JIOT.2018.2849324.

[30] P. Emami-Naeini, "Are Consumers Willing to Pay for Security and Privacy of IoT Devices?," *32nd USENIX Secur. Symp. USENIX Secur. 2023*, vol. 3, no. Query date: 2024-09-24 19:15:48, pp. 1505–1522, 2023.