The Journal of Engineering

WILEY

IET The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

A Novel Cost-Efficient Design for Electromagnetic Shielding in IoT Enclosures Against Intentional Electromagnetic Field Security Attacks

Guzlan Miskeen[1] | Mohmad Alrweg[2] | Mehdi Zeinali[2] | Alhussein Albarbar[2]

[1]Department of Biomedical Engineering, Faculty of Engineering, Wadi Alshatti University, Brak, Libya | [2]Department of Engineering, Manchester Metropolitan University, Manchester, UK

Correspondence: Mehdi Zeinali (m.zeinali@mmu.ac.uk)

Received: 20 December 2024 | **Revised:** 5 April 2025 | **Accepted:** 21 April 2025

Funding: The authors received no specific funding for this work.

ABSTRACT

The Internet of Things (IoT) has become increasingly prevalent in modern life, with connected devices permeating various aspects of daily activities. However, these IoT systems are susceptible to physical-layer attacks, wherein adversaries can exploit electromagnetic fields to compromise their security attacks. A particular concern arises from the reliance of IoT systems on the integrity of sensor signals, as these signals can be inaccurate due to manipulation by intentional electromagnetic field (IEMF) attacks. To mitigate such attacks, the implementation of effective magnetic shielding is crucial. While prior studies have recommended the use of magnetic shielding, there is a lack of research investigating its application in actively protecting IoT smart lock systems (SLSs) against tampering magnets and IEMF attacks. Increasing the thickness of shielding materials may enhance the shielding level for smart locks (SLs), but it poses challenges in terms of weight and size. Therefore, it is essential to design the shielding properly to ensure its effectiveness against both static and time-varying magnetic field attacks.

In this paper, we present a modelling approach for the magnetic shielding of a smart lock enclosure and evaluate its shielding effectiveness (SE). We developed a physical prototype of a smart lock and its protective aluminium enclosure and conducted laboratory experiments to assess the enclosure's performance against magnetic fields at various distances. The experimental data were then fed into a finite element method (FEM) numerical simulation using COMSOL to capture the impact of the distance between the SLS and the tampering magnet. The key findings demonstrate that the utilised shield can reduce the attacker's magnet power from 1/3 to 1/15 of its original IEMF field strength at the smart lock, effectively preventing it from being hacked. This shielding effectiveness was observed at distances between 5 and 25 cm, respectively.

Furthermore, the paper explores the shielding effectiveness of three enclosure materials: aluminium, stainless steel and plastic. The results show that the aluminium enclosure exhibits the highest shielding effectiveness, indicating its suitability for effectively protecting smart locks against physical attacks using tampering magnets. The proposed enclosure design can serve as a practical solution to safeguard IoT SLSs against IEMF attacks, and the findings can be extended to include user notification mechanisms for IEMF attempts.

1 | Introduction

The Internet of Things (IoT) is a networking technology that leverages the benefits of wireless sensor networks, providing adaptable, extensible and mobility-friendly platforms for communication between various devices and networks [1]. The growing popularity of IoT devices and their diverse applications has attracted the attention of adversaries, particularly those seeking to exploit the sensor functionality used in such devices through physical-layer attacks.

These IoT systems primarily rely on the integrity of input and output signals for proper operation, assuming that the sensor readings accurately represent the actual monitored phenomena or quantities, and responding accordingly [2, 3]. However, the sensor readings can be inaccurate due to manipulation [2–6]. Several studies have considered attacks that can malfunction sensors [1, 7]. One such possibility is that attackers can control IoT devices by altering the sensor data or functionality [1] through the intentional application of magnetic fields on the device's sensors, causing them to malfunction. More specifically, attackers can utilise electromagnetic waves to form intentional electromagnetic field (IEMF) attacks via the physical layer, bypassing traditional integrity mechanisms [2–6]. For instance, studies [2, 3] have investigated the feasibility of using IEMF attacks against smart locks (SLs) in IoT systems. Figure 1 depicts this scenario for a smart lock. The system is supposed to operate within the system depicted in Figure 1a. The typical system includes a broader range of functionalities. A dedicated phone application, residing on the user's smartphone, is integrated with the system via the cloud, enabling remote control and monitoring of the door status. This allows users to conveniently manage access to their premises from any location as can be seen in Figure 1.

The focus of this study is on the smart lock and its protective enclosure to provide the system with extra security to prevent tampering attempts. Figure 1b,c depicts it more clearly. In the event of a tampering attempt, the smart lock can alert the user with a suitable sensor or camera, providing an additional layer of security and enhancing the overall reliability of the system.

Figure 1a depicts the overall architecture of the smart lock system (SLS), including interactions between the smart lock, the cloud and the user's smartphone. It underlines the smart lock's connectedness to the broader IoT ecosystem. The smart lock communicates with the user via a dedicated mobile application, allowing for remote monitoring and control of the door state. The system contains multiple layers of functionality, including real-time status updates and access management. Malicious actors can exploit remote access, potentially exposing system vulnerabilities. To protect against physical-layer threats, substantial security measures, such as magnetic shielding, are necessary.

Figure 1b depicts the scenario of tampering with the smart lock via an external magnet. It demonstrates how an attacker could attempt to control the smart lock by applying an external magnet to interrupt its functionality. It also demonstrates the prospect of a direct danger to the integrity of sensor data, which might result in illegal access. The presence of a user holding the magnet serves as a visible reminder of how easily such attacks can be carried out, emphasising the crucial need for appropriate protection measures, such as increased magnetic shielding materials, to limit the effects of such tampering attempts.

Figure 1c illustrates the flow of information from the attacker to the SLS, resulting in unlawful door access. This figure effectively depicts the attacker's assault path and how purposeful electromagnetic waves might disrupt the smart lock's functionality. The sequence from attack initiation to probable illegal door opening highlights the risks in IoT systems. As a result, it is critical to incorporate advanced security protocols and protective designs, such as the suggested aluminium enclosure, that can considerably minimize the effectiveness of IEMF assaults while improving the overall security of SLSs.

The literature has suggested electromagnetic shielding or enclosures as a prevention mechanism to attenuate cyber-physical signal attacks against smart locks before they can be injected into the victim IoT devices [2–6, 10].

The use of shielding is essential in protecting the functionality of such devices [11]. However, the shape of the shield is often restricted by practical limitations, and the shielding may be only partial [12, 13].

Graphene-based polymeric composites have demonstrated superior shielding effectiveness (SE) by balancing electrical conductivity and absorption loss (SEA), particularly in lightweight, compact designs. This is essential for IoT devices requiring seamless integration with minimal weight penalties. Incorporating continuous carbon fibres and layered graphene structures into enclosure designs can significantly enhance their EMI shielding properties, ensuring device integrity in high-interference environments [14].

It is noteworthy that shielding materials provide limited protection, and a powerful attacker might still be able to breach the protection by increasing the attack power. Conductive shielding materials are suggested in the literature to eliminate electric and magnetic fields [4, 15]. Although adding thicker shielding materials can increase the shielding level, it will still challenge the device's weight and size.

Therefore, it is significantly important to design the shielding or enclosure properly to ensure its effectiveness. To this end, this work will investigate the shielding effectiveness of IoT smart lock enclosures through experimentation and simulation.

To the best of our knowledge, there is a lack of existing research that assesses the shielding effectiveness in the specific context of IoT SLSs. While adding thicker shielding materials can increase the shielding level, it also introduces challenges related to the device's weight and size.

In this paper, the evaluation of magnetic shielding is aimed at enhancing the security of smart locks. By investigating the shielding effectiveness through both experimental and simulation approaches, we seek to provide insights that can contribute to the development of a more robust and secure IoT SLSs against electromagnetic field interference (EMFI) attacks.

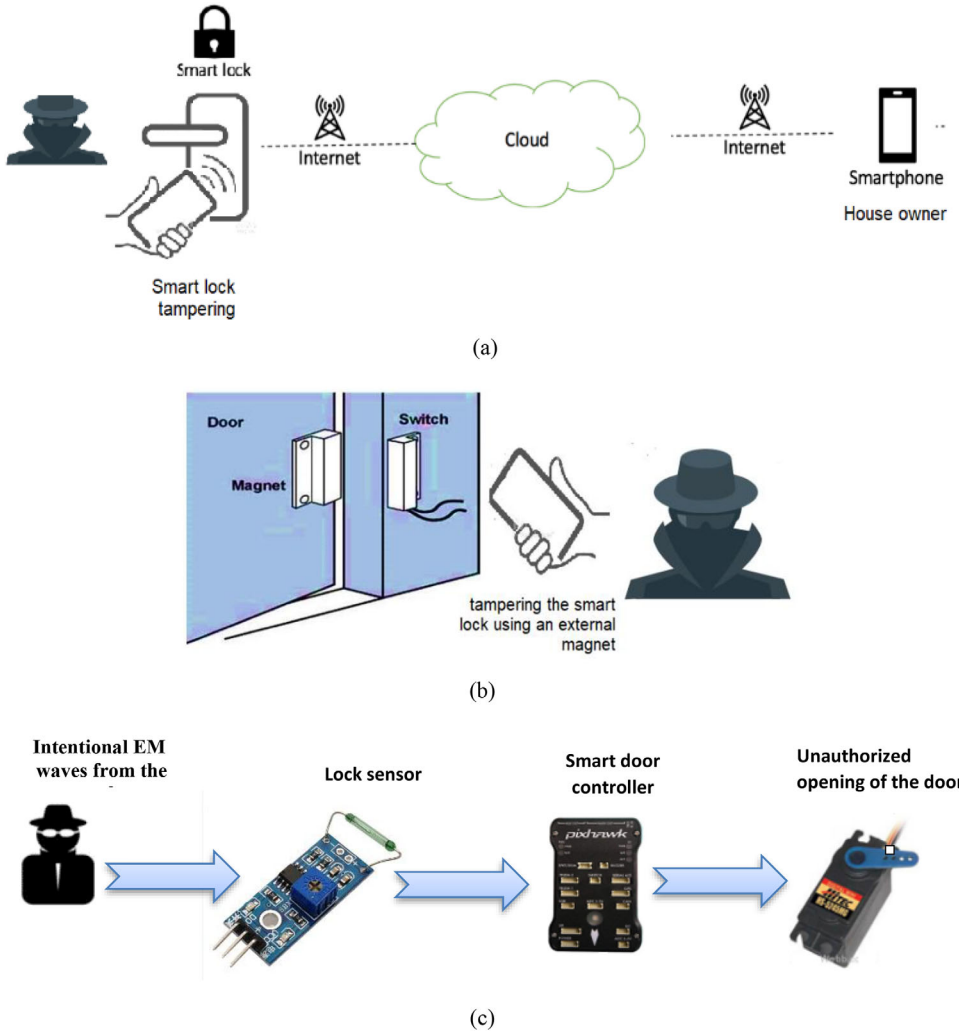

FIGURE 1 | Smart lock tampering with IEMI within IoT system (adapted from references [8, 9]).

Our key contributions to this work are as follows:

1. A novel method is presented for assessing the shielding effectiveness (SE) of IoT smart lock enclosures in the context of protection against external tampering. This method combines experimental measurements and finite element method (FEM) numerical simulations to quantify the provided protection.
2. The security level of the IoT smart lock is expressed as a function of the sensor sensitivity, providing a more comprehensive understanding of the system's protection against tampering attacks.
3. The shielding effectiveness (SE) is theoretically estimated for three enclosure materials: aluminium, stainless steel and plastic. A critical assessment is provided to evaluate the design's resilience against tampering attacks, demonstrating how SE modelling and evaluation can be integrated into the development process of IoT smart locks.
4. To the best of our knowledge, the designed and developed system is among the first in the literature to demonstrate the synergy of IoT and protective enclosures applied to implemented smart lock devices. The performance evaluation of the system offers valuable insights into its efficiency and practicality for real-world use.

By addressing these contributions, this study aims to provide guidelines for the effective implementation of shielding solutions in cyber-physical system protection.

The remainder of this paper is structured as follows:

Section 2 introduces the concept and estimation of shielding effectiveness (SE), which is a critical metric for evaluating the performance of electromagnetic shielding solutions. In Section 3, we present a review of the related work on magnetic shielding and identify the existing research gap in the context of IoT SLSs. This section highlights the need for a comprehensive investigation of shielding effectiveness in this specific application domain. Section 4 describes the system model and the settings used for the FEM numerical simulations. This section outlines the key parameters and assumptions underlying the simulation-based evaluation of the shielding performance.

2 | Smart locks and Reed sensor

2.1 | IoTs Smart Lock

Smart locks (SLs) are a type of electronic lock that can use an encrypted keypad, Bluetooth device, smartphone, WiFi or other methods to grant access to a locked door. These locks can be controlled using mobile devices or remotely through the manufacturer's servers [16]. They offer a number of advantages over traditional mechanical locks, including the ability to add or remove users without re-keying the lock and the ability to receive notifications when someone accesses the locked door [17]. One type of smart lock that has gained attention is the reed switch smart lock, which uses a magnetic field to detect whether a door is open or closed. It is vital to take into consideration the smart lock resistance against tampering and other security threats [7, 18].

2.2 | Reed Switch and Operation Concept

Reed switch is a type of electrical switch that is activated by a magnetic field and they are commonly used sensors in IoT applications [19]. Reed switches have several special features including simple design, low cost and small size. The most typical type consists of two thin ferromagnetic metal wires, known as reeds, spaced slightly apart inside a sealed glass. The switch reeds respond quickly to magnetic fields, depending on the used reed switch type (normally open [NO], normally closed [NC] or change over) [20]. Sensitivity (S) is one of the key characteristics of a reed switch. It is an indication of the amount of magnetic field required to actuate the switch and it is measured in units of ampere-turns (AT). An approximate relationship between AT, Gauss and Tesla is listed in the Appendix, and more information is available in reference [21].

In a smart lock that uses a reed sensor, the sensor is typically used to detect the position of the lock mechanism. When the lock is in the locked position, the reed sensor will detect the presence of a magnet in the lock mechanism and signal that the lock is locked (allowing current to flow in the circuit). When the magnet is removed, the contacts open, interrupting the current. This in turn will activate (trigger) an alarm and/or notify the user via an SMS or a call. However, if a strong enough tampering magnet is placed near the reed sensor, it can cause the contacts to close, even if the lock is not in the locked position. The attacker can then open the lock without needing to enter a code or use a key [7]. This is a serious security vulnerability for smart locks using reed sensors.

2.3 | IEMF Physical Attack against Smart Locks

Attacks against IoT devices can be broadly classified into three groups: attacks on the hardware (HW), attacks on the software (SW) and attacks on data in transit. Our work considers HW, more specifically; tampering alters the data associated with IoT device input within its environment [22]. Physical tampering smart locks might use magnetometer sensors or biometric sensors. Such locks could be vulnerable to tampering by cyber physical attacks. An attacker can create a fake magnetometer to fraud the targeted sensor and gain access to the smart lock. As a special case, sensor reading can be manipulated with an IEMF via the physical layer and that leads to bypassing traditional integrity mechanisms [17]. A well-known tampering attack is an intentional electromagnetic interference (IEMI) attack [2–6, 23].

3 | Shielding Effectiveness

3.1 | Enclosures Effectiveness Concept

An effective magnetic shielding should either protect a system from external fields or prevent the fields inside a system from considerably leaking to the surrounding environment [24]. One strategy for reducing magnetic fields in a specific region is to make use of material properties for altering the spatial distribution of the magnetic field from a given source [25].

There are two types of physical mechanisms used in materials-based magnetic shielding [25]:

3.1.1 | Static (Magnetostatic) Shielding

It is obtained by diverting the static magnetic flux (or DC Magnetic flux) away from the shielded region by placing a highly permeable material around the area that needs to be shielded. This material creates a preferential path for the magnetic field lines.

3.1.2 | Time-Varying (Dynamic) Magnetic Shielding

It is also known as Eddy current shielding and it is a technique used to protect against time-varying /dynamic magnetic fields. It works by inducing currents in a conductive material/shield. These induced currents generate their own magnetic field that opposes and cancels out the main, time-varying magnetic field, effectively shielding the protected area from its effects.

A quantitative measure of the effectiveness of a passive shield in reducing the magnetic field magnitude is the shielding factor or the shielding effectiveness (SE) [25]. SE quantifies the degree of isolation of a ″device/system to be protected″ [13] from an interfering electromagnetic source separated by the used obstacle/shield [10], and it can be estimated using Equation (1) [10]:

$$\mathrm{SE} = 20\mathrm{Log}_{10}(H_0/H_1) \tag{1}$$

where H_0 and H_1 are the magnetic field strength values measured without and with shielding enclosure, respectively, calculated at the electronic device position [26]. *This formula is used for both static and dynamic Magnetic Shielding estimation*.

A conducting enclosure with thickness t provides shielding effectiveness against *"dynamic Magnetic Shielding"* given by Equation (2) [10]:

$$\mathrm{SE} = \mathrm{SE_R} + \mathrm{SE_A} + \mathrm{SE_C} \tag{2}$$

Where:

SE_R: Attenuation due to reflection
SE_A: Attenuation due to absorption
SE_C: Attenuation due to multiple internal reflections. SE_A and SE_C are neglected (due to their small values)

SE_R against a time-varying/dynamic magnet in an EMFI attack can be expressed in Equation (3) [10] as:

$$SE_R = 20\,\mathrm{Log}_{10}\left\{\frac{(Z_s + Z_w)^2}{4Z_sZ_0}\right\} \tag{3}$$

Where:

Z_s: shield impedance (Ω) and it can be estimated as:

$$Z_s = 369\sqrt{\frac{\mu_r f}{\sigma_r}} \tag{4}$$

where μ_r and σ_r are the relative permeability and relative conductivity, respectively, of the enclosure material.

Z_w: wave impedance in free space (Ω)

$$Z_w = Z_0 = 120\,\pi \approx 377 \tag{5}$$

These equations will be implemented in MATLAB to assess the SE for dynamic tampering magnets with enclosures of three various materials.

3.2 | Standards on Shielding Effectiveness Measurements/Evaluation

Shielding effectiveness is an important parameter, and in practice, it is obtained through measurements [10]. Details of shielding effectiveness measurements can be found in several standards such as the Institute of Electrical and Electronic Engineers IEEE [27] and the American Society for Testing and Materials ASTM D4935-99 standard [27]. Moreover, considering the EMI and shielding, the work in reference [28] focuses on designing enclosures that can resist various environmental conditions and prevent any potential areas of leakage. This can be useful in designing an enclosure for a smart lock that includes a shield to prevent tampering with magnets. The work covers testing for any leaks, which ensures that the shield is working properly. Overall, while the work does not directly address the issue of tampering magnets, the information provided can still be applied to design an effective enclosure for a smart lock against a tampering magnet. These rules and standards help in determining the equivalent thickness of two possible enclosure materials (e.g., aluminum and plastic) [28]. The selection will be based on the obtained material thickness, the corresponding weight and other criteria, including shielding against magnet densities, material rigidity and cost. For example, an aluminium enclosure with a thickness of 5 mm will correspond to 14.62 mm of plastic [28]. An effective magnetic shield with proper material is essential to achieve high-quality factors in IoT devices.

This study follows the IEEE 299 standard for measuring shielding effectiveness (SE).

4 | Practical Considerations to Eliminate or Reduce EMC Related to IoT Locks

In the development of IoT smart locks, electromagnetic compatibility (EMC) is not merely a theoretical concern but a critical aspect of ensuring robust and secure operation in real-world electromagnetic environments. While earlier sections of this study address shielding performance through experimental and simulation-based analysis, practical implementation requires additional strategies to mitigate electromagnetic interference (EMI) at the system and circuit level. This section outlines design-level techniques—ranging from shielding and grounding practices to PCB layout and filtering considerations—grounded in established industry standards (e.g., IEEE Std 299, IEC 61000 series) [29, 30]. Together, these strategies aim to complement simulation efforts and facilitate the reliable deployment of IoT smart locks in diverse and interference-prone environments.

4.1 | EMC Solutions

To eliminate EMC issues, several strategies can be implemented:

4.1.1 | Shielding

Shielding is a fundamental technique to protect electronic circuits from external EMI. Shielding can be achieved by enclosing sensitive components within conductive materials, such as steel or aluminium, which act as barriers to block electric and magnetic fields [31]. Additionally, the effectiveness of shielding can be enhanced by ensuring proper grounding and bonding techniques are employed, which help to dissipate any induced currents and reduce the potential for interference [32].

Capacitive coupling: Shielding is essential to prevent capacitive coupling between nearby conductors. The shield should be properly grounded to ensure that noise currents are directed towards the ground. It is important to minimize the length of any wires outside the shield to avoid creating new pathways for interference [33].

Magnetic Coupling: While shielding can effectively block electric fields, special attention is required to reduce magnetic fields, especially at low frequencies. For low-frequency magnetic fields, materials like Mu-metal or permalloy are preferred, whereas copper or aluminium is more effective at higher frequencies. In high-intensity magnetic environments, multilayer shields are recommended.

4.1.2 | Grounding and Isolation

Proper grounding and isolation are essential to preventing ground loops and reducing the potential for EMI. Ground loops can introduce noise into the system, especially in circuits with both analogue and digital components.

Single-point grounding: For low-frequency applications, single-point grounding is effective in preventing ground loops. This involves connecting all ground points to a single location.

Multi-point grounding: For higher frequencies, multi-point grounding may be necessary to reduce inductive reactance in the ground system.

Isolation: Using transformers or opto-isolators can help eliminate electrical coupling and provide isolation between different sections of the circuit, thereby reducing the risk of noise interference [34].

4.1.3 | Filtering

Filters, including LC and RC circuits, serve the purpose of attenuating high-frequency noise and voltage transients that could adversely impact the functionality of IoT smart locks. Special attention should be given to the selection and placement of capacitors to ensure effective filtering.

Snubber networks, composed of resistive and capacitive elements, may be employed across electrically noisy components such as motors and relays to mitigate the effects of voltage transients and EMI.

Decoupling capacitors: These capacitors should be placed as close as possible to the power pins of ICs to filter out high-frequency noise and stabilize the power supply.

4.2 | PCB Design Considerations

The design of the PCB plays a critical role in managing EMC. The following considerations should be taken into account during PCB layout to minimize EMC issues:

Trace layout and grounding: Minimising trace lengths reduce the potential for noise pickup and radiation. Wide traces with low resistance and inductance should be used to minimize voltage drops and noise susceptibility [35].

Ground planes: Use dedicated ground planes wherever possible. In multilayer PCBs, one layer should be entirely dedicated to the ground plane, while another can be used for the power supply. This approach reduces impedance and helps contain EMI within the PCB.

Star grounding: Implementing star grounding can prevent ground loops by ensuring that all ground connections converge at a single point.

Signal integrity: Impedance matching: Ensure that the input impedance of gates and the characteristic impedance of PCB traces are matched to avoid signal reflections, which can introduce noise and interfere with the proper operation of the circuit.

Clock and signal routing: Place high-frequency clock or data transmission lines (e.g., SPI, I2C) away from sensitive analogue sections to minimise electromagnetic coupling and signal integrity degradation. Additionally, use ground lines adjacent to high-speed signals to act as a shield and reduce their impact on the rest of the circuit [36]. For example, design recommendations in [IEEE Std 299] and [IEC 61000] highlight that grounding and filtering become crucial in high-density PCB layouts typical of IoT devices.

4.3 | Decoupling and Filtering

Decoupling capacitors: It is crucial to position decoupling capacitors in close proximity to the power supply terminals of integrated circuits to effectively attenuate noise and maintain voltage stability.

Use of shielded cables: For signal lines that exit the PCB, use shielded cables to prevent external noise from coupling into the signal paths.

Incorporating these considerations during the design phase enhances the electromagnetic robustness of smart locks, ensuring compliance with industrial standards and reliable operation under real-world electromagnetic conditions even in electrically noisy environments [37].

5 | Review of Previous Work

The next subsection reviews related studies of attacks on IoT devices as well as shielding technologies for non-IoT devices.

5.1 | IEMF Attacks on IoT Devices

This section reviews research performed on IEMFs besides some other research on assessing IEMF attacks in particular on smart systems.

Considering IEMF attacks on smart systems, the work in reference [5] discussed the vulnerabilities of IoT smart locks from a cyber-physical perspective; more specifically, the threat posed by IEMF attacks against smart locks to allow unauthenticated access via lock opening without direct physical tampering via manipulating its control circuitry. The study then proposed a methodology to identify the attacks points but it did not provide a suggestion to prevent such attacks. Likewise, the work in reference [6] demonstrates that both input and output signals can be remotely manipulated via the physical layer through the use of specially created IEMI. The work showed that the physical layer signalling used in smart systems might be hacked. Three attack scenarios were analysed and their efficacy demonstrated. The interesting scenario related to this study is that the analogue sensing channel is manipulated to produce arbitrary sensor readings. Experiments showed that the attacks are effective over appreciable distances and at low power since a successful attack could occur when the attack system was placed beyond 0.5 m. Similarly, the work in reference [7] tests the performance of reed sensors in a smart lock in terms of assessing their tamper susceptibility/ resisting tampering attempts. To conduct this test, detection sensitivity was evaluated at several distances from the

sensor. The study concluded that the reed smart lock has a great detection range and exhibits a higher number of variances in its detection field. Therefore, this can be disadvantageous in security applications since they may provide opportunities for successful tampering attempts.

5.2 | IEMF Attacks on Non-IoT Devices

Considering IEMI attacks on non-IoT applications, the study in reference [3] found the impact of IEMI attacks, even with low power levels, on the functionality of power converters for electric vehicle (EV) systems. Therefore, the attackers can gain control of the EV system by manipulating the sensors' signal and can cause damage to the system partially or totally. In reference [38], SE was assessed and analysed versus EMI for metal-coated polymer materials to protect sensitive electronics from EMI. It uses an experimental setup based on the ASTM D4935-99 standard and EMI simulation using the ANSYS.

The work in reference [23] presented an approach for detecting IEMI attacks on actuator systems that usually rely on physical security measures via identifying any difference between two identical signals (the primary signal and the reference signal) as existence of manipulating attacks. The work in reference [39] presents a fast electromagnetic side channel attack against software encryption chips to obtain a security key.

5.3 | Shielding Technologies for Non-IoT Devices

Several studies in the literature have considered magnetic shielding in terms of the application context and the used shielding material. The used shielding materials differ in terms of material type, dimensions and geometry and the number of layers to specify the shielding suitably for a particular application.

For instance, the research in reference [15] measured the vulnerability of analogue sensors in implantable medical devices to signal injection attacks by intentional application of magnetic fields with varying power and distance between them and SE was not explicitly estimated in this study. A numerical simulation of SE of a shielding enclosure is carried out in reference [40] using the COMSOL FEM, verified with an experimental method based on measurement of the electric field inside the enclosure. Another study [41] investigated the most used electromagnetic shielding materials employing an Ansoft simulator to analyse the shielding performance of nickel and nickel-based materials used in protecting the circuit breaker system from outside interference. A COMSOL simulation was performed in reference [11] to evaluate and predict a magnetic field wave against a four-layer magnetic shield and SE was then estimated. Similarly, a multilayer copper and nickel-based magnetic shielding was proposed in reference [24] to protect a navigation system from external devices' magnetic fields. The performance of the designed shield was assessed via 3D COMSOL software. The research in reference [42] employed MU-metal electromagnetic shielding to mitigate crosstalk errors caused by external magnetic fields from electrical current flows, which can impair magnetic sensor functionality. However, the study did not explicitly quantify SE. The study in reference [43] simulated single- and double-layer enclosures made of recycled materials. Finally, as a different approach, the work in reference [44] utilises machine learning (ML) to predict the shielding effectiveness of carbon fibres using frequency and mixed design parameters.

5.4 Research Gap

According to the surveyed studies, the following research gaps were identified:

In the context of the magnetic shielding application for IoTs, to the best of our knowledge, none of the previous studies have estimated via experiment or simulation the shielding effectiveness in IoT devices in smart home applications, despite the spread of the smart sensors usage for domestic building applications.

The current study aims to model and simulate a shielded smart lock against EMIF. More specifically, this paper presents a method to quantify the effectiveness of smart lock enclosures against EMIF attacks. In addition, the work also developed a physical prototype of a smart lock and protective enclosure. It also provides both lab experiments and FEM simulations of an aluminium enclosure against a magnetic field at several distances. The study also provides a theoretical estimation of the shielding effectiveness for three different enclosure materials: aluminium, stainless steel and plastic. While the mathematical formulas and use of COMSOL for shielding simulation are not novel, the research contributes by investigating the shielding of smart locks against external tampering magnets and assessing the level of protection provided.

6 | The Proposed Model: The Implemented Smart Lock and Enclosure

6.1 | Model Description

We developed a physical prototype of a smart lock and its corresponding enclosure and then evaluated the effectiveness of the enclosure using FEM simulations. The overall methodology is summarized in the smart lock system testing process shown in Figure 2. The underlying idea is to use magnetic shielding within the enclosure to protect the magnetometer in the smart lock from the impacts of electromagnetic field interference (EMFI).

The system was constructed and the corresponding shield was made of aluminium with predefined dimensions to fully enclose the system while adhering to relevant standards and guidelines [28]. The thickness and material of the shield were selected to provide an adequate shielding factor suitable for the SLS application, ensuring sufficient protection. The chosen geometry and dimensions of the shield were determined based on the dimensions of the lock board. Experiments were conducted to estimate the shielding effectiveness at various distances, mimicking the effect of varying wall thicknesses. In the COMSOL simulation, the resulting magnetic fields without shielding were applied to model the impact of distance variations on the magnetic field density. Figure 3 depicts the block diagram of the proposed SLS design, which includes a magnetometer/reed switch sensor,

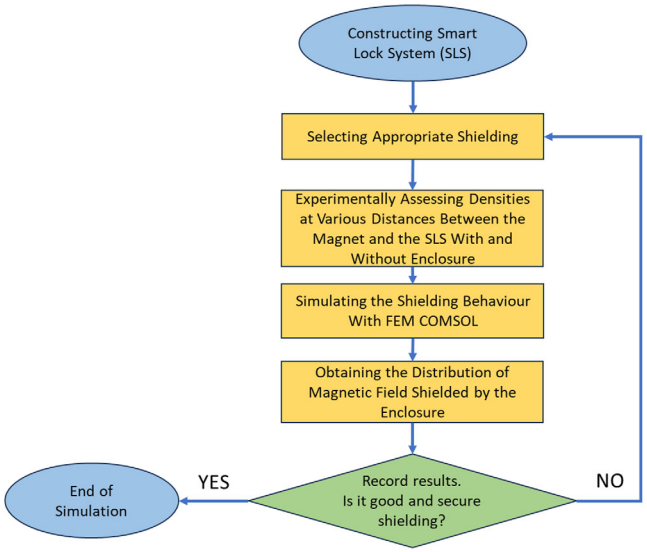

FIGURE 2 | The process of the smart lock system simulation and testing.

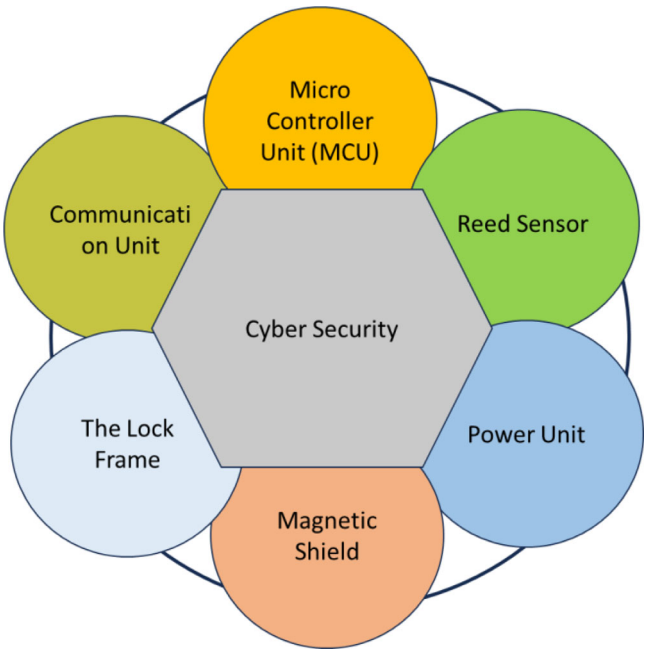

FIGURE 3 | The block diagram of the main components of the smart lock system.

microcontroller, power unit, radio frequency (RF) unit and cyber security at the top of all the components, to investigate the effect of the magnetic field on the system.

6.2 | Shield Design

The aluminium shield was designed to provide additional protection to the magnetometer. The shield was then implemented with the dimensions listed in Table 1. Figure 4 illustrates the final smart locks and the shape of the proposed shield.

TABLE 1 | The design details of the protecting shield.

Material type	Aluminium
Dimensions (mm)	$30 \times 60 \times 3$
Number of layers	1
Thickness (mm)	3
Presence of holes	—
Geometry shape	Rectangular

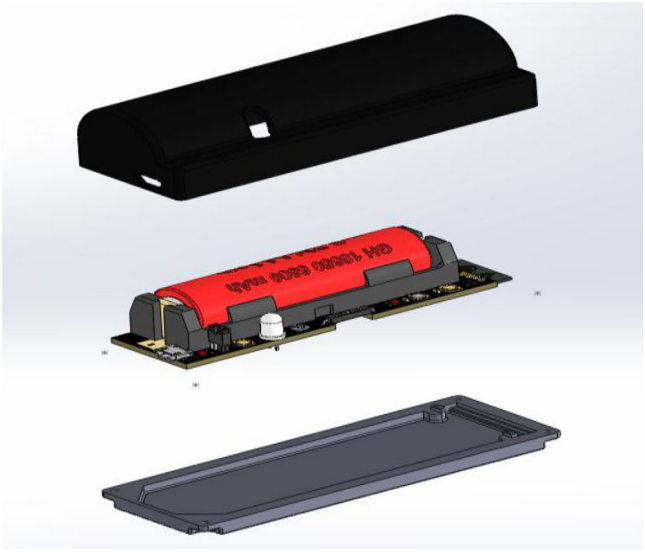

FIGURE 4 | The implemented smart lock and the corresponding shield.

TABLE 2 | The specifications of the magnet used in the experiment.

R (mm)	L (mm)	B_r (T)	H (T)
5	60	30	0.1396613

6.3 | Empirical Assessment: Shield Effectiveness Estimation/Measurement (Static Tampering Magnetic Fields)

This research employed an empirical approach to estimate the shielding factor. A Tesla meter (Model 5180) [45]. The impact of wall thickness was investigated by varying the distance between the magnet and the designed enclosure. The measured magnetic density without the shield served as input for the COMSOL simulation software. This methodology aligns with the approach presented in reference [46] for empirically determining shielding effectiveness (SE). The magnetic field was measured at various distances, both with and without the shield present. Subsequently, SE was calculated using Equation (4). Magnetic field density measurements were taken at distances ranging from 5 to 25 cm, encompassing the maximum thickness of the shield (25 cm). These values were then used in the COMSOL simulation. The experiment utilised a cylindrical neodymium magnet with a magnetic field of 0.1396613 T, whose characteristics are detailed in Table 2.

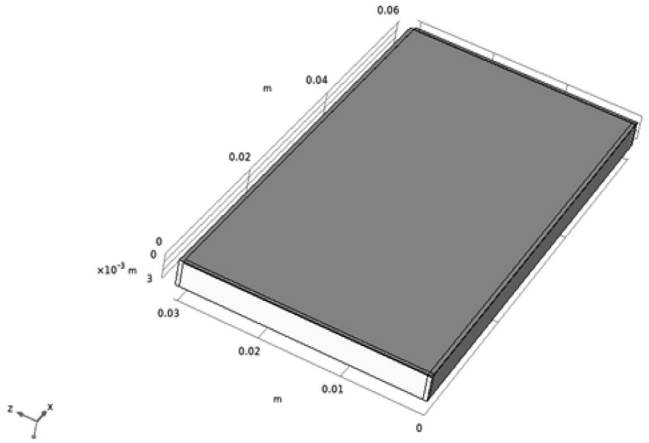

FIGURE 5 | 3D COMSOL Model for smart lock system shield.

6.4 | COMSOL Model

Numerical methods, such as those employed using COMSOL software, offer a practical and cost-effective alternative to theoretical calculations and experimental investigations when determining the shielding effectiveness (SE) of various designs [24]. COMSOL, a 3D simulation software utilising the FEM, can analyse complex systems of partial differential equations. Notably, it can numerically solve for magnetic fields in the presence of arbitrarily shaped magnetic materials [47]. This research leveraged COMSOL version 5.5 to investigate SE by simulating the magnetic density resulting from applying an intentional electromagnetic field (IEMF) to the shield designed for the smart lock. Transition magnetic shield boundary conditions were applied to the geometry, enabling the evaluation of the proposed shielding's effectiveness based on the distribution of the magnetic field both inside and outside the shield.

Accurate boundary conditions are crucial for obtaining reliable simulation results. The model boundary was implemented as a perfect match layer (PML) to enhance the transition of the source signal [40, 47]. The shield/enclosure is approximated as a perfect electric conductor (PEC), that is:

$$\vec{n} \times \vec{E} = 0 \tag{6}$$

The shield's boundary is modelled as a PEC when the enclosure material is highly conductive. This boundary condition implies that both the electric and magnetic field components parallel to the boundary are zero. PEC boundaries are perfectly reflective, preventing any energy from escaping the simulation volume through that boundary [40]. The definition of the source within the simulation depends on the chosen method. For the FEM, it is possible to directly incorporate a magnetic field source. The accuracy of the solution is considered good when the total electric energy remains constant regardless of the number of degrees of freedom (DOFs) [47]. The proposed shield for the smart lock, designed using COMSOL, is illustrated in Figure 5. Detailed information regarding the Maxwell equations and boundary conditions used for the shield is provided in the Appendix.

TABLE 3 | The conductivity and permeability of the tested enclosure materials.

Enclosure material	Conductivity σ_r	Permeability μ_r
Aluminium	0.601	1.000022
Stainless steel	0.02	1.003
Plastic	8.62×10^{-6}	1.79

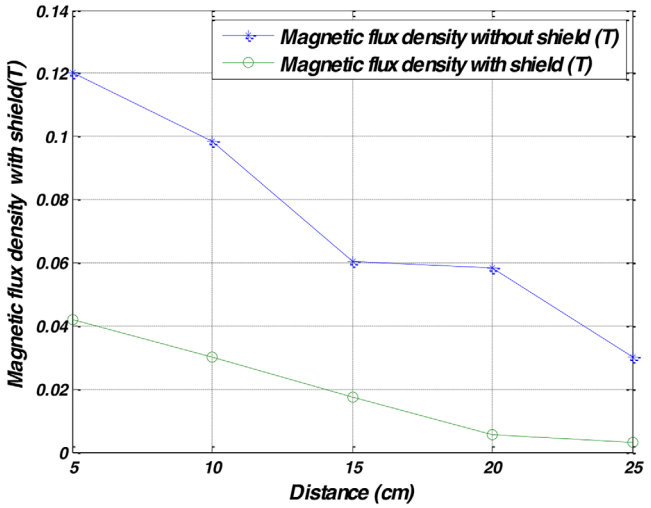

FIGURE 6 | The shielding effect on the magnetic flux density against distance (obtained via experiment).

6.5 | Shield Effectiveness Estimation (Dynamic Tampering Magnetic)

The estimation of SE, for a dynamic tampering magnet, where its frequency is varied, is based on a set of equations ranging from Equations (5) to (8). The conductivity and permeability values used for aluminium, stainless steel and plastic enclosures are obtained from reference [48] and are listed in Table 3.

7 | Results, Comments and Discussions

7.1 | Estimating SE via FEM Experiment

This section presents the experimental results for magnetic density measurements, both with and without the shield, as summarised in Table 4. These results demonstrate the effectiveness of the proposed shielding. At a distance of 5 cm, the shielded signal exhibited a reduction of approximately 9 dB, effectively requiring an attacker to apply three times the magnetic field strength to achieve the same impact on the SLS. This signifies a three-fold reduction in the magnetic field's influence (in the worst-case scenario). The shielding factor increases to 15 times at a distance of 25 cm (in the best-case scenario). The measured non-shielded magnetic density values were compared with theoretical calculations based on Equation (2), as shown in Table 4. Figure 6 illustrates the experimental results for the magnetic field with the proposed shield. A linear relationship between distance and magnetic field strength is evident in both shielded and unshielded cases. The presence of the shield significantly reduces

TABLE 4 | Experimental measuring of the magnetic field against the distance with and without the shield.

Distance (cm)	Magnetic flux density without shield (Tesla)	Magnetic flux density with shield (Tesla)	Shielding Effectiveness SE (dB)
5	0.1203	0.04194	9.15
10	0.09838	0.029908	10.34
15	0.06051	0.01756	10.75
20	0.058203	0.005572	20.38
25	0.030126	0.002938	20.21

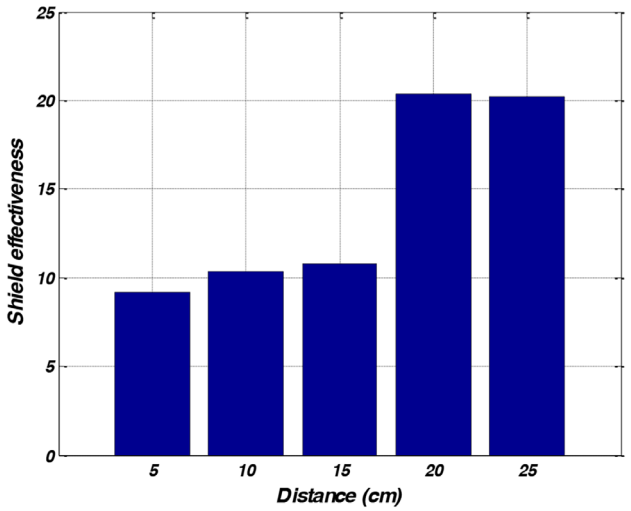

FIGURE 7 | Shielding effectiveness factor against distance (obtained via experiment).

the magnetic flux to approximately one-third of its original value. The experimental results indicate that the simple, single-layer shield achieves a shielding factor of approximately 20.

To facilitate the prediction of shielding effectiveness (SE) for varying distances, linear regression models were applied to the data presented in Figure 6 for both shielded and unshielded cases.

$$\textbf{Without shielding}: \quad y = -0.00441x + 0.14 \quad R^2 = 0.955 \tag{7}$$

$$\textbf{With shielding}: \quad y = -0.002047x + 0.05029 \quad R^2 = 0.966 \tag{8}$$

where x represents the distance (in centimetres) between the smart lock and the magnet, while y denotes the magnetic flux density (in Tesla). The relationship between distance and magnetic flux density is inversely proportional, indicating a linear decrease in magnetic flux density with increasing distance. The regression coefficients were determined using the least squares method (LSM). The R^2 values for the models are 0.955 and 0.9663, respectively, indicating a high degree of accuracy in estimating magnetic flux density at a given distance.

Figure 7 depicts the empirical estimation of the shielding effectiveness (SE) factor based on the data presented in Table 5. The results of the SE estimation through simulation will be discussed in the subsequent section.

TABLE 5 | Comparing the experimental and theoretical magnetic field (according to Equation 2; without shielding).

Distance (cm)	Experimental magnetic flux density (Tesla)	Theoretical magnetic flux density without shield (Tesla)
5	0.1203	0.120792
10	0.09838	0.104735
15	0.06051	0.070885
20	0.058203	0.061694
25	0.030126	0.032769

7.2 | Estimating SE via FEM COMSOL Simulation

Figure 8a–d illustrates the magnetic field intensity distribution on the proposed metal shield of the IoT smart lock when subjected to magnetic flux from various distances (5, 10, 15, 20, and 25 cm) from the aluminium shield. Notably, the maximum values of magnetic flux density are observed at the shield edges. This phenomenon can be attributed to the lower permeability of air compared to the shield material. The designed shield effectively prevents the penetration of the magnetic wave across most of the enclosure's shielded areas. As the distance between the magnetic field source and the shield increases, the magnetic field density decreases.

From Figure 9, it is obvious that the designed shield is capable of providing a higher shielding factor at closer distances, particularly at the centre of the shield. This enhanced protection at close distances is crucial for safeguarding the magnetometer from external tampering magnetic fields. The simulated SE values obtained from the 3D model show good agreement with the experimentally measured SE values, as presented in Table 6 and Figure 9.

The experimental and simulation results clearly demonstrate the significant impact of distance on reducing the strength of the tampering magnet used in EMFI attacks as can be seen in Table 7. For instance, at a distance of 5 cm, the magnetic flux is 60 times

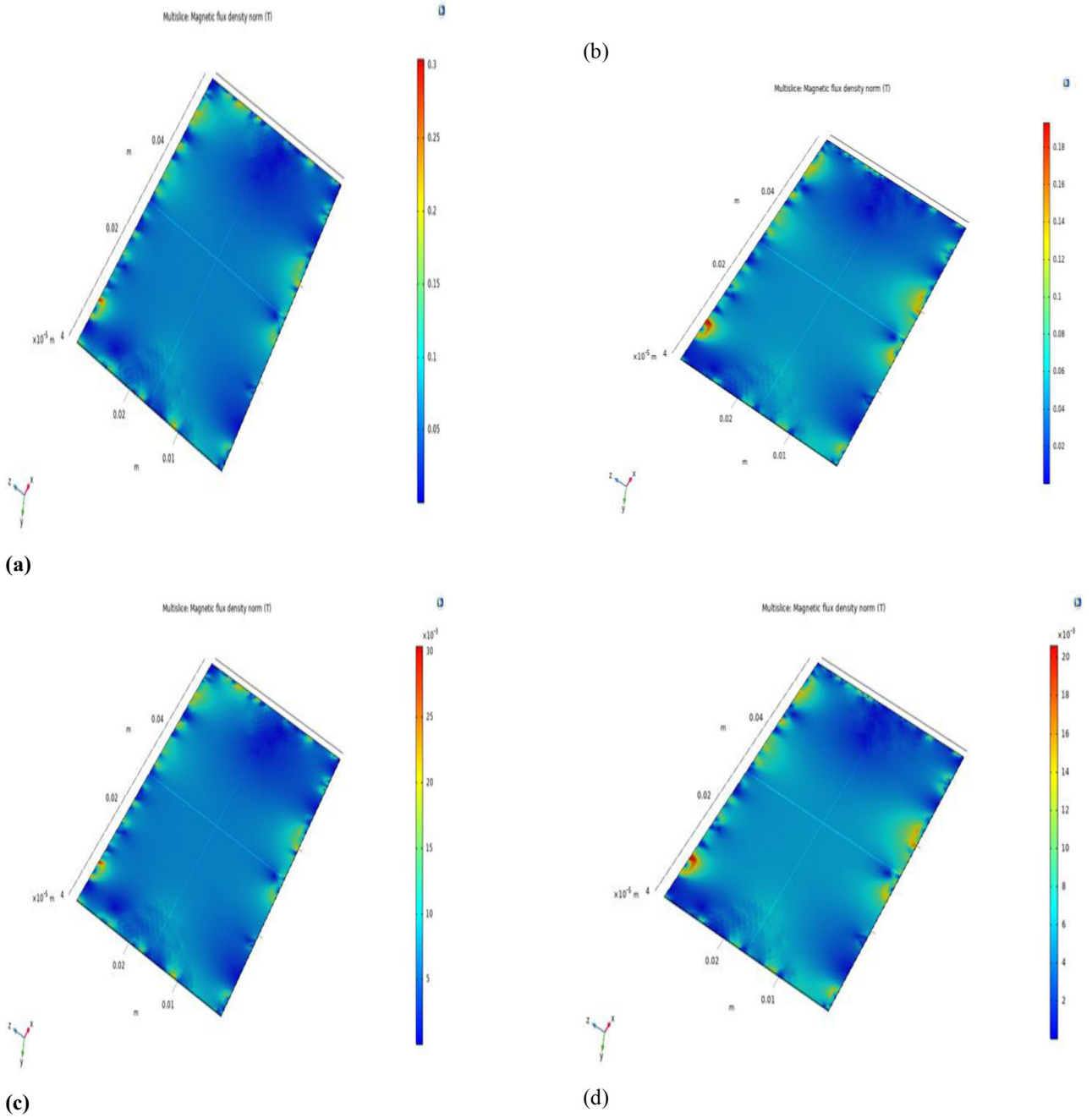

FIGURE 8 | The magnetic flux density (at different distances from the shielding enclosure side: (a) 5 cm; (b) 10 cm; (c) 15 cm; (d) 20 cm).

TABLE 6 | The applied magnetic field values (without shield) for COMSOL simulation and the corresponding estimated output for various distances.

Distance (cm)	Applied magnetic flux density without shield (Tesla)—in COMSOL simulation	Estimated magnetic flux density with shield (Tesla) Via COMSOL simulation	Distance (cm)
5	0.1203	0.04221	5
10	0.09838	0.02873	10
15	0.06051	0.01690	15
20	0.058203	0.00531	20

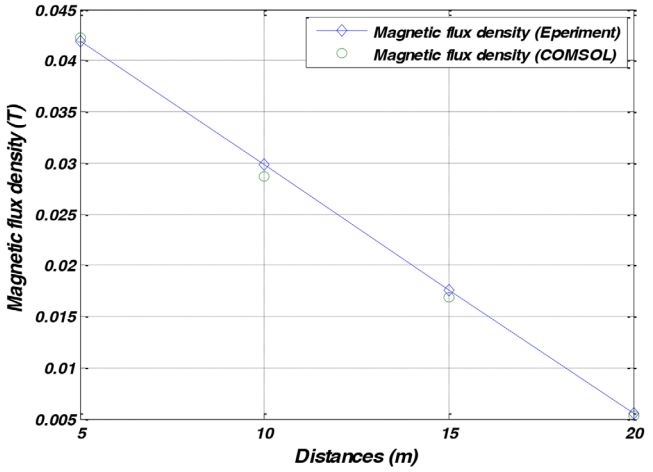

FIGURE 9 | Comparison of experiment and COMSOL simulation for the magnetic field against the distance with the shield.

TABLE 7 | Comparison of experiment and COMSOL simulation for the magnetic field against the distance with the shield.

Distance (cm)	Magnetic flux density with shield (Tesla): Experiment	Magnetic flux density with shield (Tesla): COMSOL
5	0.04194	0.04221
10	0.029908	0.02873
15	0.01756	0.01690
20	0.005572	0.00531

greater than the sensor sensitivity, while at 25 cm, it is only 15 times greater. The proposed shield effectively reduces the strength of the tampering magnet further. For instance, at a distance of 5 cm, the shield reduces the magnetic field to approximately 21 times the sensor sensitivity, compared to its original strength. At 25 cm, the shield reduces the strength to 1.5 times the sensor sensitivity, as detailed in Table 8.

These findings confirm that the proposed shield significantly reduces the likelihood of unauthorised door opening through IEMF attacks, assuming the magnet is properly oriented. This additional layer of protection further enhances the security of SLSs, minimising the risk of malfunctions.

7.3 | Impact of Magnet Material on SE

Figure 10 illustrates the impact of enclosure material on shielding effectiveness. Aluminium demonstrates the highest shielding effectiveness compared to plastic and stainless steel, while also offering the advantages of being lightweight and sufficiently rigid to provide adequate protection for the smart lock. The shielding effectiveness (SE) was estimated using Equation (3), assuming a dynamic magnet with a frequency of 10^5 Hz.

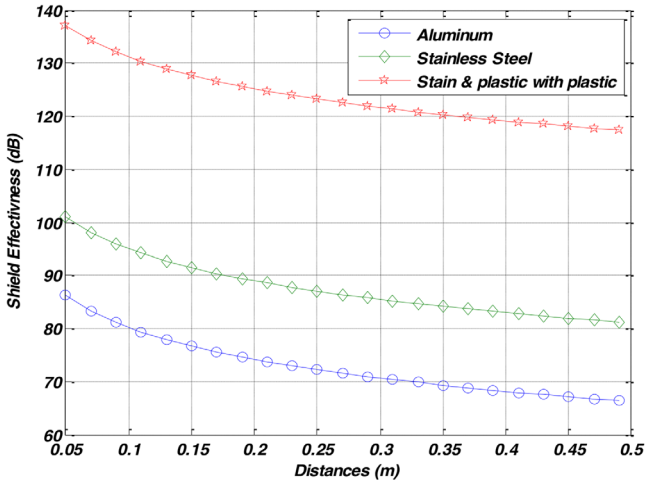

FIGURE 10 | Shield effectiveness for different enclosure materials at tampering magnet frequency 10^5 Hz and various distances.

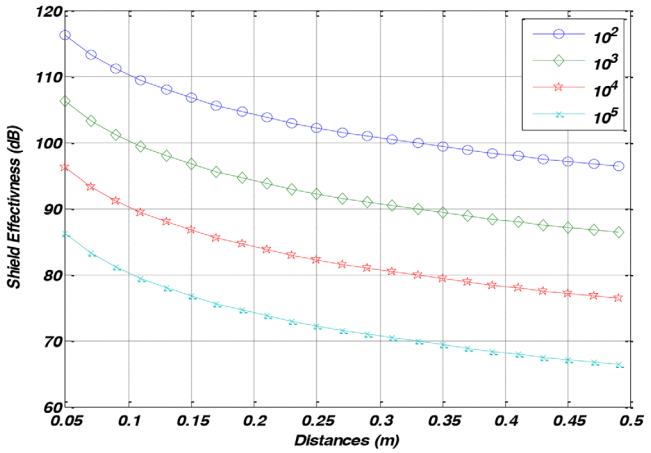

FIGURE 11 | Shied effectiveness for an aluminium enclosure at various tampering magnet frequencies and distances.

The obtained results indicated the effectiveness of the shield in reducing the magnetic field strength at various distances, effectively mitigating the impact of tampering magnets.

7.4 | Impact of Frequency of Dynamic Tampering Magnet on SE

Figure 11 depicts the impact of the tampering magnet frequency on shielding effectiveness. The higher the frequency, the lesser protection the enclosure provides. The shielding effectiveness (SE) was estimated using Equation (3), assuming a dynamic magnet with a frequency varying from 10^2 to 10^5 Hz.

8 | Conclusions and Future Work

This work presented a novel approach for modelling the magnetic shielding behaviour for IoT smart locks against EMFI attacks.

The study focuses on the design and evaluation of a magnetic shield for an SLS, aiming to protect the device from external tampering using magnets. The proposed aluminium shield was

TABLE 8 | The comparison between the effects of distance vs. adding extra protection to the reed sensor via the proposed shield.

Distance (cm)	Magnetic flux density without shield (T)	Magnetic flux density with shield (T)	Average reed sensor sensitivity multiples (with no shielding)	Average reed sensor sensitivity multiples (with shielding)
5	0.1203	0.04194	60.15	20.97
10	0.09838	0.029908	49.19	14.95
15	0.06051	0.01756	30.26	8.78
20	0.058203	0.005572	29.10	2.79

designed and evaluated through a combination of FEM simulations and laboratory experiments. The results demonstrate the effectiveness of the shield in reducing the magnetic field strength at various distances, effectively mitigating the impact of tampering magnets. The obtained results of the FEM simulation/experiment model can be utilised in the context of protecting smart locks from external magnets to provide actively secure systems. In terms of sensor sensitivity, the research concludes that the proposed shield reduces the risk of opening the door using an EMFI magnet from 60 times the sensor sensitivity at 5 cm to only 15 times the sensor sensitivity. This demonstrates the significant impact of the shield in reducing the vulnerability of the smart lock to EMFI attacks. Furthermore, the study compared the shielding effectiveness of aluminium, stainless steel and plastic enclosures. The results indicate that aluminium provides the highest shielding factor, making it the most suitable material for protecting smart locks against physical attacks using tampering magnets.

Additionally, some practical strategies to eliminate or reduce the EMI for IoT smart lock design, including PCB design techniques, shielding and grounding, have been outlined to enhance the resilience of the device against EMI.

The study suggests further investigation into the impact of various parameters on shield effectiveness, including the number of layers, the presence of gaps between layers, the type of magnetic shield and the strength of the external magnet. These insights will contribute to the development of more robust and effective shielding solutions for securing SLSs against EMFI attacks.

Author Contributions

Guzlan Miskeen: conceptualisation, formal analysis, investigation, methodology, validation, writing – original draft. **Mohmad Alrweg:** conceptualisation, formal analysis, investigation, methodology, validation, visualisation, writing – original draft. **Mehdi Zeinali:** visualisation, writing – original draft. **Alhussein Albarbar:** writing – review and editing.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The data supporting the findings of this study are available upon reasonable request from the corresponding author. Restrictions may apply to the availability of some data due to privacy or ethical considerations.

References

1. B. Asad and N. Saxena, "On the Feasibility of DoS Attack on Smart Door Lock IoT Network," in Security in Computing and Communications: 8th International Symposium, SSCC 2020, Chennai, India, October 14–17, 2020, Revised Selected Papers, vol. 8 (Springer, 2021), 123–138.

2. G. Y. Dayanikli, "Electromagnetic Interference Attacks on Cyber-Physical Systems: Theory, Demonstration, and Defense" (PhD diss., Virginia Tech, 2021).

3. G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles," in Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW) (IEEE, 2020), 98–103.

4. Y. Zhang, "Electromagnetic Signal Injection Attacks on Embedded Systems: Modeling and Detection" (PhD diss., University of Oxford, 2022).

5. A. Z. Mohammed, A. Singh, G. Y. Dayanikli, R. Gerdes, M. Mina, and M. Li, "Towards Wireless Spiking of Smart Locks," in Proceedings of the 2022 IEEE Security and Privacy Workshops (SPW) (IEEE, 2022), 251–257.

6. J. Selvaraj, G. Y. Dayanikli, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic Induction Attacks Against Embedded Systems," in Proceedings of the2018 Asia Conferenceon Computer and Communications Security (Association for Computing Machinery, 2018), 499–510.

7. A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A Survey on Sensor-Based Threats and Attacks to Smart Devices and Applications," *IEEE Communications Surveys & Tutorials* 23, no. 2 (2021): 1125–1159.

8. A. Dabhade, T. Javare, A. Ghayal, Shelar, and A. Gupta, "Smart Door Lock System: Improving Home Security using Bluetooth Technology," *International Journal of Computer Applications* 160, no. 8 (2017): 1922.

9. M. S. Hadis, E. Palantei, A. A. Ilham, and A. Hendra, "Design of Smart Lock System for Doors With Special Features Using Bluetooth Technology," in Proceedings of the 2018 International Conference on Information and Communications Technology (ICOIACT) (IEEE, 2018), 396–400.

10. L. Sevgi, "Electromagnetic Screening and Shielding-Effectiveness (SE) Modeling," *IEEE Antennas and Propagation Magazine* 51, no. 6 (2009): 211–216.

11. Y. Zhao, Z. Sun, D. Pan, S. Lin, Y. Jin, and L. Li, "A New Approach to Calculate the Shielding Factor of Magnetic Shields Comprising Nonlinear Ferromagnetic Materials Under Arbitrary Disturbances," *Energies* 12, no. 10 (2019): 2048.

12. M. Jaroszewski, S. Thomas, and A. V. Rane, *Advanced Materials for Electromagnetic Shielding: Fundamentals, Properties, and Applications*. 1st ed. (CRC Press, 2018).

13. A. Keshtkar, A. Maghoul, and A. Kalantarnia, "Magnetic Shield Effectiveness in Low Frequency," *International Journal of Computer and Electrical Engineering* 3, no. 6 (2011): 507–513.

14. J. T. Orasugh and S. S. Ray, "Functional and Structural Facts of Effective Electromagnetic Interference Shielding Materials: A Review," *ACS Omega* 8, no. 9 (2023): 8134–8158, https://pubs.acs.org/doi/epdf/10.1021/acsomega.2c05815?ref=article_openPDF.

15. D. F. Kune, J. Backes, S. S. Clark, et al., "Ghost Talk: Mitigating EMI Signal Injection Attacks Against Analog Sensors," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (IEEE, 2013), 145–159.

16. G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart Locks: Lessons for Securing Commodity Internet of Things Devices," in Proceeding of the 11th ACM Asia Conference. Comput. Commun. Security (Association for Computing Machinery, 2016), 461–472.

17. C. Caballero-Gil, R. Alvarez, C. Hernández-Goya, and J. Molina-Gil, "Research on Smart-Locks Cybersecurity and Vulnerabilities," *Wireless Network* 29, no. 4 (2023): 1503–1516.

18. N. Krishnamoorthy, R. Kalaimagal, S. G. Shankar, and N. A. Asif, "IoT Based Smart Door Locks," *International Journal on Future Revolution in Computer Science & Communication Engineering* 4, no. 5 (2018): 151–154.

19. S. Tumanski, "Modern Magnetic Field Sensors–A Review," *Organizing* 10, no. 2 (2013): 1–12.

20. R. S. Components Ltd., "Reed Switches Guide," 2020, https://uk.rs-online.com/web/generalDisplay.html?id=ideas-and-advice/reed-switches-guide.

21. M. Pickhard, "Advantages of Reed Switch Technology for Low-Power Metering Applications," *Fierce Electronics* (2014), https://www.fierceelectronics.com/components/top-five-advantages-reed-switch-technology-for-low-power-metering-applications.

22. P. Williams, H. Daoud, and M. Bayoumi, "A Survey on Security in Internet of Things With a Focus on the Impact of Emerging Technologies," *Internet Things* 19, no. 3 (2022): 45–68.

23. Y. Zhang and K. Rasmussen, "Detection of Electromagnetic Signal Injection Attacks on Actuator Systems," in Proceeding of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID) (2022), 171–184.

24. J. Wu, "Compact Magnetic Shielding Using Thick-Film Electroplated Permalloy" (PhD diss., University of California, 2020).

25. O. Bottauscio, *2D and 3D Magnetic Shielding Simulation Methods and Practical Aspects* (Istituto Elettrotecnico Nazionale Galileo Ferraris, 2005).

26. R. Armstrong, "Measurement of Shielding in Electrically Large Metallic Enclosures" (PhD diss., University of York, 2013).

27. IEEE Standard, *IEEE STD-299-1997: IEEE Standard for Measuring the Effectiveness of Electromagnetic Shielding Enclosures*, (IEEE, 1997).

28. T. Serksnis, *Designing Electronic Product Enclosures* (Springer, 2019).

29. IEEE Std 299–2006, "IEEE Recommended Practice for Measurement of Shielding Effectiveness of High-Performance Shielding Enclosures", https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4117954.

30. IEC 61000 SER, "Electromagnetic Compatibility (EMC)", IEC61000-3:2025SERvElectromagneticcompatibility(EMC).

31. W. Chen, "1. Recent Advances in Electromagnetic Interference Suppression," *Highlights in Science Engineering and Technology* 71 (2023): 221–226, https://doi.org/10.54097/hset.v71i.12698.

32. D. Demaratos, "Method for Shielding and Grounding Connector From Electromagnetic Interference Using Conductive Seal and Housing," (2020), Methodforshieldingandgroundingaconnectorassembly fromelectromagneticinterference(EMI)usingconductivesealand conductivehousing.

33. L. Bo, R. Ren, W. Fei, C. Daniel, and Z. Zheyu, "6. Capacitive Coupling in EMI Filters Containing T-Shaped Joint: Mechanism, Effects, and Mitigation," *IEEE Transactions on Power Electronics* 35, no. 3 (2020): 2534–2547, https://doi.org/10.1109/TPEL.2019.2934478.

34. J. Li and C. Liao, "Ground Bounce Noise Isolation With Power Plane Segmentation in System-in-Package (SiP)," in Proceedings of the International Conference on Microwave Millimeter Wave Technology (IEEE, 2007), 381–388.

35. J. Tian, "Reducing Electromagnetic Interference in Printed Circuit Boards," in Proceedings of the IEEE International Conference on Applications of Communications Engineering (ICAPC) (IEEE, 2022), 66–73.

36. M. Zeinali, PCB Layout Rules, Comprehensive Technical Report to R&D Department (Saghif Eng. Co., 2008).

37. Q. Liu, S. Wang, A. C. Baisden, F. Wang, and D. Boroyevich, "EMI Suppression in Voltage Source Converters by Utilizing DC-link Decoupling Capacitors," *IEEE Transactions on Power Electronics* 22, no. 4 (2007): 1410–1419.

38. S. J. Mostafavi Yazdi, A. Lisitski, S. Pack, H. R. Hiziroglu, and J. Baqersad, "Analysis of Shielding Effectiveness Against Electromagnetic Interference (EMI) for Metal-Coated Polymeric Materials," *Polymers* 15, no. 6 (2023): 1911.

39. W.-H. Zhou and F.-T. Kong, "Electromagnetic Side Channel Attack Against Embedded Encryption Chips," in Proceedings of the 2019 IEEE 19th International Conference on Communications Technology (ICCT) (IEEE, 2019), 140–144.

40. Z. Kubík and J. Skála, "Shielding Effectiveness Simulation of Small Perforated Shielding Enclosures Using FEM," *Energies* 9, no. 5 (2016): 129.

41. L. Conecici, C. Munteanu, and I. Purcar, "Study of the Shielding Performances of Different Materials Regarding Electromagnetic Field Interference," *IOP Conference Series: Materials Science and Engineering* 163 (2017): 012045.

42. A. MicroSystems, "Reducing the Influence of External Fields and Crosstalk for Contactless Current Sensing," (2020), Currentsensorsystem.

43. A. Jakubas, E. Łada-Tondyra, Ł. Suchecki, and M. Makówka, "Simulations and Tests of the Effectiveness of Electromagnetic Field Shielding by Shields Made of Recycled Materials," *Przegląd Elektrotechniczny* 98, no. 5 (2022): 33–41.

44. S. Narayanan, Y. Zhang, and F. Aslani, "Prediction Models of Shielding Effectiveness of Carbon Fibre Reinforced Cement-Based Composites Against Electromagnetic Interference," *Sensors* 23, no. 4 (2023): 2084.

45. Scientific Technologies, "Model 5170/5180 Gauss/Tesla Meter Instruction Manual," (2018), Model5170/5180.

46. C. Morari and I. Balan, "Methods for Determining Shielding Effectiveness of Materials," *Electrotehnica, Electronica, Automatica* 63, no. 4 (2015): 126–135.

47. A. B. Comsol, "COMSOL Multiphysics," Version 6.1, Stockholm, Sweden (2021).

48. R. Evans, "Design Guidelines for Shielding Effectiveness, Current Carrying Capability, and the Enhancement of Conductivity of Composite Materials" (PhD diss., National Aeronautics and Space Administration, 1997).

49. First4Magnets, "Reed Switch," (2020), https://www.first4magnets.com/blog/what-is-a-reed-switch-and-which-magnets-operate-them/.

50. B. Adamczyk, *Foundations of Electromagnetic Compatibility: With Practical Applications* (John Wiley & Sons, 2017).

A | Sensitivity of the Used Reed Switch

Sensitivity (S) is a key characteristic of reed switches. An approximate relationship between AT, Gauss and Tesla is listed in the Appendix and more information is available in reference [21]:

$$1\ \mathrm{AT} = 1\ \ \mathrm{Gauss} = 0.1\ \ \mathrm{milli} - \mathrm{Tesla}\ \ (\mathrm{mT}) \tag{A1}$$

The sensitivity of the used reed switch is in the range of 18 to 22 AT, that is, from 18 to 22 mT [20, 21]. For instance, if the tempering magnet type is a neodymium cylinder magnet, its magnetic field of 0.1396613 T is around 77.5 times the reed sensor sensitivity to consider a worst scenario. The

magnetic field strength H (in Tesla) of a cylinder magnet can be estimated at distance x according to the following formula [49]:

$$H = \frac{B_r}{2}\left[\left(\frac{L+x}{\sqrt{r^2+(L+x^2)}}\right)-\left(\frac{x}{\sqrt{r^2+x^2}}\right)\right] \quad \text{(A2)}$$

where:

B_r: The remanence of the magnet (Tesla)
r: the radius of the magnet
L: the length (thickness) of the magnet
x: the distance between the magnet and the shield

The minimum strength of the magnet that actuates the reed switch is:

$$H_{\min} = S \quad \text{(A3)}$$

In this case and from Equations (A.2) and (A.3), the relationship between the sensitivity of the reed switch and the distance and the magnet dimensions can be written as [21]:

$$\mathrm{S} = \frac{B_r}{2}\left[\left(\frac{L+x}{\sqrt{r^2+(L+x^2)}}\right)-\left(\frac{x}{\sqrt{r^2+x^2}}\right)\right] \quad \text{(A4)}$$

8.2Maxwell Equations and Boundary Conditions for FEM Simulation

In this section, **Maxwell** equations and **boundary conditions** for rectangular enclosures are listed. The electromagnetic field distributions on the enclosure surfaces can be obtained from Maxwell equations [50]:

$$\nabla.\vec{D} = q_e \quad \text{(A.1)}$$

$$\nabla\times\vec{E} = \frac{\partial\vec{B}}{\partial t} \quad \text{(A.2)}$$

$$\nabla.\vec{B} = 0 \quad \text{(A.3)}$$

$$\nabla\times\vec{H} = \vec{J} + \frac{\partial\vec{D}}{\partial t} \quad \text{(A.4)}$$

where $\vec{B}$ and $\vec{H}$ are magnetic induction and magnetic field intensity, respectively; $\vec{E}$ and $\vec{D}$ are, respectively, electric field intensity and electric displacement; q_e and $\vec{J}$ are, respectively, the free charge density and the free current density. Let $\vec{n}$ represent a unit vector that is normal to the surface S of the enclosure, then the boundary conditions for an electromagnetic field are:

$$\vec{n}.\vec{D} = q_s \quad \text{(A.5)}$$

$$\vec{n}\times\vec{E} = 0 \quad \text{(A.6)}$$

$$\vec{n}.\vec{B} = 0 \quad \text{(A.7)}$$

$$\vec{n}\times\vec{H} = J_s \quad \text{(A.8)}$$

q_s and J_s are, respectively, the surface charge density and the surface current density. where $\vec{B}$ is estimated as:

$$\vec{B} = \mu_0\mu_r\vec{H}$$

μ_0 is the permeability in vacuum; μ_r is the relative permeability of the enclosure material.