A Survey on Enhancing the Security of Data Transmission in IoT Healthcare Devices

|  |  |  |  |
| --- | --- | --- | --- |
| *Yetunde Mary Adeyemo*  *Manchester Metropolitan University*  *Manchester, UK*  *23632147@stu.mmu.ac.uk* | *Meekness Chiagoziem Friday*  *Manchester Metropolitan University*  *Manchester, UK*  *23700209 @stu.mmu.ac.uk* | | *Deepak Gowda Nilavadi Rajamudi*  *Manchester Metropolitan University*  *Manchester, UK*  *23703617 @stu.mmu.ac.uk* |
| *Samuel Fikayo Akinyemi*  *Manchester Metropolitan University*  *Manchester, UK*  *23728303@stu.mmu.ac.uk* | | *Azeez Boluwatife Abdullahi*  *Manchester Metropolitan University*  *Manchester, UK*  *23713593 @stu.mmu.ac.uk* | |

***Abstract -* The growing adoption of the Internet of Things in healthcare has led to the advent of linked medical devices that monitor and collect data to improve patient care. The sensitive nature of personal health information requires strict data transmission security in Internet of Medical Things contexts. This paper aims to analyze security measures aimed at improving the transmission of data in IOT healthcare devices.** **This paper classifies the security measures into two main categories 1) Data Pre-processing Techniques for Data Efficiency and 2) Encryption Algorithms for Secure Data Transmission. It analyses Dynamic Lightweight Symmetric, Blowfish, Discrete Decision Tree Hashing, Rivest Cypher, Elliptic Curve Digital Signature, and Secure Hash algorithms to determine how they protect data confidentiality, integrity, and authenticity. Innovations like using Ant Colony Optimisation to improve hashing and using Blowfish for digital certificates demonstrate the multidimensional approach to IoMT security. Agile healthcare data preprocessing to fix discrepancies, combine datasets, and normalize inputs to improve security is detailed. We critically evaluate security-device performance trade-offs using encryption efficiency and system overhead. Moreover, we also provided more information on the challenges related to effective data transmission in IOT healthcare, as well as the evaluation tools used to measure the performance of the system.**

***Keywords: IoT healthcare devices, data security, cryptographic algorithms, data preprocessing, IoMT security, secure data transmission.***

1. INTRODUCTION

The fast rise of the Internet of Things (IoT) is altering various industries, including healthcare, by fostering connectivity and communication. In this networked environment, IoT healthcare gadgets provide real-time data transfer, remote monitoring, and innovative patient care. The authors in [3] analyze the importance of the Internet of Things (IoT) in several fields, with a specific focus on healthcare, where it has transformed into the Internet of Medical Things (IoMT). Seamless data exchange between medical devices and healthcare systems enhances the accuracy of diagnosis, effectiveness of therapy, and overall patient outcomes.

Nevertheless, the growing use of Internet of Things (IoT) devices in the healthcare sector presents significant security concerns, particularly with the transfer of data. [3] stated that IoT sensors are susceptible to several types of attacks due to their capacity to record and send sensitive information. Therefore, it is crucial to employ strong cryptographic algorithms to guarantee the confidentiality, integrity, and availability of patient data while it is being sent. Protecting data flow in IoT healthcare equipment requires understanding the increasing threat landscape's complicated concerns.

This study examines the Internet of Medical Things (IoMT) device data preprocessing, security methods, and encryption. By highlighting gaps in the present framework and studying cutting-edge technologies, we seek to aid efforts to secure data transfer in this critical sector. This survey research explored healthcare data transmission security methods in detail under classification. The classes also list potential security measures. In addition to a quick assessment of data transmission security, this study discusses future research issues and concerns.

This paper's organization continues below. IoT is briefly explained in Section 2. Section 3 provides an overview and review of healthcare data transfer security. Section 4 discusses problems, and Section 5 describes performance evaluation techniques. Finally, Section 6 concludes our survey paper.

1. INTERNET OF THINGS: A BRIEF OVERVIEW

Interconnectivity of devices through the use of the Internet is what is meant by the term "Internet of Things" (IoT). Devices can range from commonplace items to sophisticated instruments, and everything in between. Users can obtain greater degrees of automation, analysis, and integration inside a system through the usage of Internet of Things (IoT) platforms, which significantly improves their reach and accuracy. The Internet of Things makes use of both established and developing technologies, including sensing, networking, and robotics, among others.

Software, sensors, and other technologies are already being embedded into commonplace items like appliances, automobiles, and clothing. These technologies enable these objects to collect and share data. The phenomenon that is in question is referred to as the Internet of Things (IoT), and it has a significant influence on your life. It has the potential to enhance productivity, convenience, and cost-effectiveness.

You can remotely operate your home, monitor your fitness and health, and streamline industrial processes with the help of the Internet of Things. On the other hand, the extensive level of connectivity and the sharing of data creates concerns regarding privacy and security. It is of the utmost importance to know both the advantages and the difficulties associated with this technology. The current number of linked Internet of Things devices is 7 billion, but experts anticipate that this number will increase to 10 billion by the year 2020 and 22 billion by the year 2025.

The Internet of Things (IoT) empowers devices to autonomously execute repetitive tasks, hence decreasing expenses, minimizing inefficiencies, and enhancing the quality-of-service provision. It enhances the cost-efficiency and transparency of manufacturing and delivering items to customers. The Internet of Things (IoT) has emerged as a highly influential technology in the 21st century. Using embedded devices, it is possible to establish effective communication between individuals, processes, and objects by connecting common items like kitchen appliances, healthcare devices, thermostats, and baby monitors to the Internet.

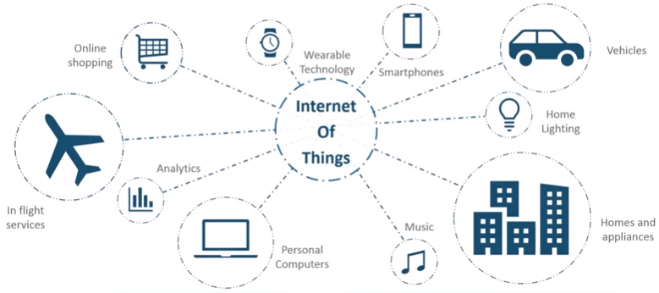


Fig 1. Internet of Things Framework

Source: Adapted from [8]

# SECURITY MEASURES FOR HEALTHCARE DATA TRANSMISSION

Healthcare data transmission within the Internet of Things (IoT) requires advanced security measures to keep sensitive medical information confidential, secure, and available. The focus of this discussion is on the integration of robust cryptographic algorithms such as Dynamic Lightweight Symmetric (DLS), Blowfish algorithm (BA), Discrete Decision Tree Hashing Algorithm (DDTHA), Rivest Cipher (RC6), Elliptic Curve Digital Signature Algorithm (ECDSA) and Secure Harsh Algorithm (SHA256) to enhance data transmission security from medical devices and the data pre-processing technique that was used to enhance the security. In the following sections, we discuss how the proposed system enhances the security of healthcare data.

1. *Data Pre-processing Technique for Data Efficiency*

Data preprocessing is regarded as one of the most important classifications for improving data security in healthcare IOT devices. The basis of data preprocessing in IoT stems from the need to modify sensor-generated data that is frequently plagued with flaws such as noise, missing values, outliers, and inconsistencies. Preprocessing is, therefore, the important precursor to any significant data analysis or mining, seeking to improve data quality and enable reliable conclusions.

The classification of data preprocessing approaches addressed in the paper [6], according to the author, revolves around four important categories: data cleaning, data integration, data transformation, and data reduction, with each addressing distinct challenges faced in IoT data sets. This part of preprocessing focuses on data cleaning, which attempts to challenge and correct erroneous or incomplete data items. Data cleaning techniques include everything from simple deletion strategies to advanced imputation techniques. List-wise and pairwise deletions, for example, give simple methods for dealing with missing data, but other types of imputation—deductive, mean, median, mode, random sampling, regression, and multiple imputation—provide more subtle methods for inferring missing values.

A diagram of data processing

Description automatically generated

Fig 2. Four Steps in Data Preprocessing

Source: Adapted from [7]

The review [6] also highlights the crucial importance of data integration, a process that combines information from disparate sources into a coherent dataset, providing a single view of the data environment. The paper makes use of coupling methods and ETL (Extraction, Transformation, and Loading) procedures to reconcile discrepancies across multiple data sources, maintaining integrity and streamlining analysis.

The preprocessing framework stated in [6] includes other pillars such as data transformation and data reduction. Smoothing, aggregation, normalization, and discretization are transformation procedures that convert raw data into a structured and processable format that is frequently tuned to the characteristics of the analytical model at hand. These solutions reduce the volume of IoT data while solving computing and storage problems and focusing on analytic accuracy.

In [2], normalisation was used as another type of data preprocessing technique. To begin, health data collected from IoT devices is normalised to remove irrelevant or redundant data from raw datasets. When the data is processed by the security improvement model in the study [2], the normalisation process improves the quality of the datasets, resulting in more dependable outcomes. The use of normalisation in data preprocessing is important in the execution of the suggested improved security model in [2]. The normalised data is subsequently employed in the application of an optimised hashing technique, which is then further processed by digital certificates for authentication purposes.

The Mobile Health (M-Health) dataset, which comprises vital signs and body movements of 10 persons conducting diverse physical activities, is used in the article [3]. Sensors on the wrist, ankle, and chest are used to collect data. The data is then analysed to discover errors, missing values, and corrupted records in the following stage of the process. Missing values are restored by computing the mean or median of the non-missing values or by employing the K-nearest neighbour imputation (kNNI) approach. Principal Component Analysis (PCA) is a data reduction approach used to control the size and complexity of the dataset. PCA is a statistical process that employs an orthogonal transformation to turn a set of possibly correlated observations into a set of values of linearly uncorrelated variables known as principal components. For feature extraction, the study in [5] uses a Modified Local Binary Pattern. This operation establishes a threshold by using a pixel as a centre point and converting the grey value to a binary code. This efficiently decreases the dimensionality while retaining the necessary information for future processing.

1. *Encryption Algorithms for Secure Data Transmission*

When it comes to the Internet of Things (IoT) and healthcare data transfer, using encryption methods is essential to protecting private and sensitive medical data while it is being transmitted. The encryption algorithm for secure data transmission protects data while it travels from one point of access (PoA) to another, much like the relocation of a server node's content in a purely wired network like the Internet. For example, let us consider a situation in which medical data is comparable to a valuable server located at a particular region. The encryption algorithm, which is responsible for protecting this data, is essential in ensuring that it is securely transferred from implanted medical devices to the intended receiver while Algorithms like DLS, BA, DDTHA, RC6, ECDSA, and SHA256, This classification aims at understanding the complexities of these cryptographic techniques, assessing their efficacy and application for strengthening security infrastructure as well as ensuring that healthcare data is protected against potential threats and unauthorised access. Further sections, which will shed light on the features of encryption algorithms and their vital contribution towards a larger objective to increase security, shall be provided.

An algorithm for secure data transmission is crucial for maintaining the privacy and integrity of information sent across networks. In [1], the authors suggest using Dynamic Lightweight Symmetric (DLS) encryption to achieve secure data transmission in Body Sensor Networks (BSNs). DLS employs a basic function like XOR to encrypt data at the sensor node, creating unique temporal encryption keys. This method, specifically designed for resource-limited BSNs, strikes a balance between security and efficiency. However, there are certain limitations to this proposed approach. One disadvantage is the reliance on generating distinct encryption keys for each message transmission, making the security of the DLS algorithm vulnerable if an attacker gains access to the secret key or random number used in key generation. Moreover, the DLS algorithm, designed with a focus on small data sizes, may not be well-suited for applications involving the transmission of substantial amounts of data.

The second encryption algorithm chosen for ensuring secure data transmission is Blowfish as shown in Fig 1. The proposed scheme utilizes the Blowfish algorithm to transform plain text into cipher text, ensuring both the confidentiality and integrity of the transmitted data. Blowfish is a symmetric-key block cipher that processes data in 64-bit blocks with a variable-length key of up to 448 bits. Its operational mechanism involves multiple iterations of a substitution-permutation network, providing a robust level of security and efficiency in encrypting data.

In [2], the authors employ Ant Colony Optimisation in an Internet of Things (IoT) based healthcare system, combining a Discrete Decision Tree Hashing Algorithm (DDTHA). An important part of data authentication is DDTHA's hashing algorithm for unsigned digital certificates. Recall, precision, and specificity are some of the factors used in its one-of-a-kind hashing algorithm and objective function. It is observed that this method yields greater values in comparison to current techniques, suggesting a more secure hashing process. Conversely, ACO is implemented to enhance the hash function's operational efficiency. The programme uses ant colony behaviour for deposition and reacting to pheromone trails, to identify the best option. By reducing processing time while increasing performance, ACO acts as an effective solution. To add another degree of protection, the suggested method uses the Blowfish technique to encrypt data using signed digital certificates.

In [2], the authors advocate for the use of the Blowfish algorithm to encrypt data and generate signed digital certificates for authentication, thereby enhancing data transmission security in healthcare applications. However, a potential disadvantage of the proposed scheme is its specific focus on heart problems, suggesting a limited scope in addressing a broader range of healthcare issues. To enhance applicability in healthcare data transmission and security, there is a need for further expansion to encompass a more diverse set of medical conditions.

A diagram of data processing

Description automatically generated

Fig. 3. The proposed methodology for Blowfish Algorithm. Source: Adapted from [2]

The suggested system facilitates secure data transmission in Internet of Medical Things (IoMT) devices by combining several encryption algorithms. several encryption techniques are used as part of the system's working mechanism to guarantee the availability, confidentiality, and integrity of sensitive medical data.

In [3], The authors proposed the RC6 algorithm which is a symmetric key block cipher that generates a key value, it serves as a crucial component in the encryption process. It is used to encrypt the patient's medical details in the medical repository.   
It guarantees data confidentiality by transforming information into an unintelligible format that can solely be deciphered with the corresponding key. Subsequently, In [4] the ECDSA (Elliptic Curve Digital Signature Algorithm), proposed by Johnson et al., is utilized to encrypt the key value obtained from RC6. ECDSA (Elliptic Curve Digital Signature Algorithm) It manages remote access to patient data by employing a public-private key pair.

The private key signs the message, while the public key verifies the signature, ensuring data authenticity and thwarting unauthorized access. In this context, it is used to encrypt the key value, thereby enhancing the security of the data transmission process. After encrypting with ECDSA, the encrypted result output undergoes a hashing step using the SHA256 algorithm, as recommended by the National Institute of Standards and Technology (NIST). Secure Hash Algorithm 256-bit (SHA256) is a cryptographic hash function that produces a cryptographic hash function that generates a fixed-size output (256 bits) from any input data. Through the use of SHA256, the system boosts the integrity and authenticity of transmitted data, guaranteeing that the information stays unchanged during both transmission and storage.

The encrypted algorithms (RC6, ECDSA, SHA256) work together to provide a robust approach and a very strong security measure for data transmission in the IoMT system. They ensure that the data is protected from unauthorized access and other security threats that may occur. It has some limitations. One of the limitations is the significant increase in the size of the encrypted message. Additionally, the use of short passwords with the SHA-256 algorithm poses a vulnerability, as such passwords can be more easily identified by potential attackers. These limitations highlight the need for ongoing refinement and optimization of the encryption mechanisms to address potential vulnerabilities and enhance the overall security of the system.

1. RESEARCH CHALLENGES
2. *Data Quality and Integration*

One acknowledged weakness in [5] is the k-Nearest Neighbours algorithm's reliance on the quality of training data during the data cleaning stage. The classification accuracy may be impaired if there are major mistakes in the data labeling or if the training data contains noise and artifacts. The reliability of KNN-aided preprocessing is dependent on high-quality and precisely labeled data. As a clarification of the previous point, the KNN method is sensitive to mislabeled or conflicting sample groups in the training data, which can lead to decreased classification reliability.

1. *Performance of the System*

Concerns are raised in [3] concerning the efficiency of hardware with greater key lengths. While this is not a direct constraint, it may signal possible challenges in combining security with system performance. [1] analyses the suggested technique's performance implications, taking into account aspects such as memory usage, processor overhead, and power consumption, which may restrict its application to specific devices or circumstances.

1. EVALUATION TOOLS

Various simulation and evaluation tools are available to measure the performance of data transmission in IOT healthcare, such as MATLAB [5] and the use of Python as the programming language and an Intel processor as the computational platform. The analysis in [5] focused on performance indicators such as packet delivery ratio, energy usage, throughput, network lifetime, and packet loss. MATLAB simulations were employed to compare the suggested methodologies with established protocols like the routing protocol for low-power networks (RPL) and the connecting tree protocol (CTP). The simulations confirmed that the proposed Butter Ant Optimisation (BAO) algorithm effectively reduces end-to-end delay, energy consumption, and packet loss, and improves network lifetime, packet delivery ratio, and throughput to a significant extent.

Python and an Intel CPU were used in [3] for the experimental analysis. Encryption and decryption were stimulated in Python and performance-tested on an Intel processor. This method assessed healthcare service throughput, packet loss, time, and memory speedup, and secure data transfer in the Internet of Medical Things (IoMT). Python was used for modeling and experimentation on an Intel processor. ECG audio signal encryption and decryption time were assessed using RC6, ECDSA, and SHA256 security algorithms. The network throughput was assessed by dividing an input file by the number of encryption or decryption units.

1. CONCLUSION

This survey paper has provided a comprehensive analysis of the security challenges and advancements in the transmission of data within IoT healthcare devices. It emphasizes the significance of using strong encryption algorithms like DLS, Blowfish, DDTHA, RC6, ECDSA, and SHA256 to protect sensitive medical data during transmission and storage. The research also emphasises the need for data pre-processing to improve data quality and efficiency, which is crucial to security model reliability. The paper acknowledges the need for ongoing research to address the limitations and optimize the performance of these security measures, particularly in the context of expanding the scope of healthcare conditions covered and improving system efficiency. This survey paper serves as a valuable resource for understanding the current state of IoT healthcare device security and points toward future directions for research.

REFERENCES

1. *S. Banani, S. Thiemjarus, K. Wongthavarawat, and N. Ounanong, “A Dynamic Light-weight symmetric encryption algorithm for secure data transmission via BLE beacons,” J. Sens. Actuator Netw., vol. 11, no. 1, p. 2, 2021. (references)*
2. *A. M. Al Shahrani, A. Rizwan, M. Sánchez-Chero, C. E. Rosas-Prado, E. B. Salazar, and N. A. Awad, “An Internet of Things (IoT)-based optimization to enhance security in healthcare applications,” Math. Probl. Eng., vol. 2022, pp. 1–7, 2022.*
3. *S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri, and S. Alkhalaf, “Secure data transmission in the internet of medical things using RES-256 algorithm,” IEEE Trans. Industr. Inform., vol. 18, no. 12, pp. 8876–8884, 2022*.
4. *D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, 2001.*
5. *E. Refaee et al., “Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications,” Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–12, 2022.*
6. *V. Jane. "Survey on IoT Data Preprocessing". Turkish Journal of Computer and Mathematics Education (TURCOMAT). vol. 12. no. 9. pp. 238-244. Apr. 2021.* [*https://doi.org/10.17762/turcomat.v12i9.3001*](https://doi.org/10.17762/turcomat.v12i9.3001)*.*
7. *P. Baheti, A Simple Guide to Data Preprocessing in Machine Learning. 2021. [Online]. Available:* [*https://www.v7labs.com/blog/data-preprocessing-guide*](https://www.v7labs.com/blog/data-preprocessing-guide)*.*
8. *M. Akram, IoT Decision Framework. 2021. [Online]. Available: https://medium.com/@MohamedWasim001/iot-decision-framework-407cf81cf*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. **Mark** | **86 – 100 (Outstanding)** | **70 – 85 (Excellent)** | **60 – 69 (Good)** | **50 -59 (Acceptable)** | **1-49 (Poor)** |
| **Abstract (10%)** | Concise, clearly outlines aim of study, methodology, findings, and conclusions | Strong writing in relation to motivations/ideas, approaches, and results of the report | Summary of the report in relation to motivations and ideas, approaches, and results of the report in all aspects | Summary of most aspects, such as motivations/ideas, approaches, and the results of the report | Incomplete description/summary regarding motivation/ideas, approach, and results of the paper  Missing abstract. |
| **Introduction (15%)** | Introduces topic  Clear, logical progression from literature review to aims of study  Choice of methodology introduced and supported  Aims and hypotheses well formulated | Clear presentation of the topic.  Methodology of survey discussed.  Aims and hypotheses at least touched upon. | Topic introduced but not fully explained.  Methodology of survey discussed.  Limited reference to aims, objectives or outcome of the survey. | Survey topic introduced but unclear to reader.  Methodology presented with limited clarity.  Very limited or no reference to aims, objectives or outcome of the survey. | Some attempt to introduce the topic of the survey.  Little or no description of the survey methodology.  Failure to adequately introduce the surveyed topic. |
| **Survey Body (30%)** | All materials are relevant to the objectives of the study.  Shows in-depth understanding of the techniques, methodology, and mechanisms described in the reading materials  Provide synthesis and critical analysis of previous research and its relation to the current study  Excellent coverage of the surveyed topic and evaluation tools. | Materials are relevant to the objectives of the study.  Shows sufficient understanding of the techniques/ methodology/ mechanisms described in the reading materials  Provide sufficient synthesis and critical analysis of previous research and its relation to the current study  Very good coverage of the surveyed topic and evaluation tools. | Majority of materials are relevant to the objectives of the study.  Shows some understanding of the techniques/ methodology/ mechanisms described in the reading materials  Provide some synthesis and critical analysis of previous research and its relation to the current study  Reasonable coverage  of the surveyed topic and evaluation tools | Some materials are relevant to the objectives of the study.  Shows some understanding of the techniques/ methodology/ mechanisms described in the reading materials  An attempt at critical analysis and synthesis of the surveyed papers.  Weak coverage of the survey topic and evaluation tools | Few materials are relevant to the objectives of the study.  Shows limited understanding of the techniques/ methodology/ mechanisms described in the reading materials  Provides limited synthesis and critical analysis of previous research and its relation to the current study |
| **Conclusion (10%)** | Clear presentation of fully justified findings.  Logical conclusions based on research evidence.  Critical competence. | Logical conclusions  Predominantly based on evidence.  Evidence of ability to critically evaluate.  Results linked consistently to objectives. | Clear presentation of conclusions related to evidence.  Results linked to objectives of the study. | Draws together some of the ideas from the survey.  Results mostly linked to objectives of the study. | Weak conclusions.  Little or no conclusions drawn. |
| **Macro-Structure (15%)** | Clear and informative title  Very effective organisation using the format specified.  Divided into appropriate sections (Intro, Method, etc.)  Headings and subheadings informative  References are complete and correctly cited in the text and bibliography  Very effective use of language with accuracy in syntax, grammar, and mechanics, making explanations clear and coherent.  Very wide variety of appropriate word choices. | Clear title  Effective organisation using the format specified.  Divided into appropriate sections and subsections  Headings and subheadings appropriate  References complete and correctly cited in text and bibliography with few omissions  Effective use of language with mostly accurate syntax, grammar, and mechanics, making explanation clear and coherent.  Wide variety of appropriate word choice. | A clear title  Well organised using the format specified.  Good use of sections and subsections with appropriate naming.  Good referencing.  Good use of language with accuracy in syntax, grammar, and mechanics, making explanation clear and coherent.  Some variety of appropriate word choice. | Acceptable title.  Organisation approaches the expected format.  Limited use of headings and subheadings, or sections and subsections poorly labelled.  Good referencing, perhaps with minor errors.  Acceptable use of language: writing is readable and coherent, with perhaps minor errors. | Title does not capture the topic being surveyed.  Poor organisation, ignoring expected format.  Headings/subheadings poorly chosen or missing.  Missing sections. Missing references,  deviations from the specified referencing style, errors in referencing.  Poor use of language with limited accuracy in syntax, grammar and mechanics, making some parts of explanation incomprehensible and incoherent.  Limited word choice. |
| **Self-Reflections (20%)** | An annotated copy with supporting comments and a link with evidence. | A copy of the marking grid with a bullet point for each annotation, easy to read and organised.  Evidence of an honest self-reflection. | A copy of the marking grid with some supporting comments but unorganised explaining how they have met that grade boundary. | Annotated copy of the marking grid without any supporting comments. | No annotated copy of the marking grid |