International Journal of Computer Science and Information Technology Research (IJCSITR)
Vol. 5, No. 2, July - December, 2024, pp. 114-134
Journal ID: 9471-1297; DOI: https://doi.org/10.63530/IJCSITR_2024_05_02_010
website: www.ijcsitr.com

Automated Patch Management for Endpoints: Ensuring Compliance in Healthcare and Education Sectors

Anjan Gundaboina
Senior DevsecOps and Cloud Architect, USA.

Abstract

Automated patch management has become a critical factor in an organisation's security compliance plan and is perhaps more essential in industries such as the healthcare sector and education due to sensitive information. In the context of this article, we widen our understanding of patch management and describe an original, general approach to an automated patch management system as a solution for endpoint protection. Here, we highlight the issues with compliance with rules and regulations such as Healthcare in Information Technology, HIPAA (Health Insurance Portability and Accountability Act), and FERPA (Family Educational Rights and Privacy Act). It also evaluates the practices that are currently being used, their issues and why there is a need to automate the process to fix them. This new model also involves patch deployment procedures, ongoing compliance checks and endpoint health checks. This roughly entails the use of machine learning in deciding the prioritisation of patches and risk analysis. Employing practical datasets concerning both sectors, the effectiveness of the proposed approach was shown. We determined that we have accumulated 45% in assimilation of notable vulnerabilities within the least amount of time and decreased compliance violations by 32%. Finally, the issue of potential future work is discussed and includes the development of AI-enabled patch testing and the decentralised verification of compliance solutions.

Keywords

Patch Management, Compliance, Healthcare IT, HIPAA, FERPA, Automation, Machine Learning.

How to Cite: Anjan Gundaboina. (2024). Automated Patch Management for Endpoints: Ensuring Compliance in Healthcare and Education Sectors. *International Journal of Computer Science and Information Technology Research (IJCSITR)*, 5(2), 114-134.
DOI: https://doi.org/10.63530/IJCSITR_2024_05_02_010

Article ID: IJCSITR_2024_05_02_010

1. Introduction

As the endpoints evolve and become more complicated devices in the organisation's network, they become more susceptible to attacks, and hence, the organisations must consider preventive measures. Hospitals, schools, clinics, colleges, universities and other learning institutions possess a lot of personal and protected information of their clients. [1-4] Infringements in these areas are not just a violation and loss of information, but also legal consequences and customer mistrust.

1.1. Importance of Patch Management

Patch management is one of the significant processes that offer protection to the IT framework of an organisation from intrusions, bugs, and typical glitches that may cause the system to fall short of regulatory policies. In that regard, organisations can protect their systems by ensuring that they are up to date with security patching, updates and fixes. The post is about patch management covers many domains, starting with information protection and ending with strict compliance and has significant importance in enterprise instances as well as at institutional levels.

- **Enhancing Security Posture**: A major concept that is associated with the practice of patch management is the strengthening of the organisation's security protection measures. Specifically, patches are fixes for certain issues that exist in operating systems, applications, and devices perhaps susceptible to exploitation by hackers. Unpatched systems are said to be vulnerable to malware, ransomware, and other malicious elements in the system. It will also help the organisations to keep the

vulnerabilities fixed and reduce the attack surface for any security breaches at any time. When patch management is not efficiently done, organisations act as sitting ducks to attacks, loss of data, and the worst is the severe financial repercussions it attracts.

- **Compliance with Regulatory Standards**: It is, therefore, a legal requirement that organisations in various sectors such as healthcare, education, finance, and the government adhere to regulatory standards. Governmental policies like HIPAA require organisations to be secure, and one of such measures is ensuring constant patching of software. This approach to patch management enables organisations to meet these compliance requirements to avoid various consequences such as penalties, fines or even legal repercussions. Real-time tracking and documentation: It enables the organisation to track and document all patching activities in real-time for auditing and compliance checks.
- **Minimising System Downtime**: There are still vulnerabilities which can result in system failures or security breaches that may affect its operations, hence leading to downtimes. Ransomware, for instance, targets unpatched vulnerabilities, making it difficult for organisations to manage since they have to spend hours trying to restore their systems from the attack. On the other hand, the timely patching of the issues can reduce such incidents with a focus on maintaining the operations of the systems and services running without interruption. Procedures for routinely patching should be done during off-business hours because doing so helps decrease business inconveniences while ensuring that systems are running as they should.
- **Reducing Operational Risks**: To be effective, patch management is not only about external risks but also those threats that can occur internally and happen operationally. The computers with unpatched vulnerabilities could exhibit less than desirable performance due to bugs in new software, issues with other programs or declines in speed and efficiency. Such misrepresentation in operations can affect overall functioning and organisational goals for the business. Add to expenses, and demotivate its clients. This is because organisations can be able to protect their IT systems from being slowed down or even crashing due to outdated software by updating them.
- **Improving Incident Response and Recovery**: Patch management is incredibly

important in the management of incidents and the rectification process. Thus, ensuring that systems are kept up to date is relevant because organisations shall be in a position to prevent and respond to acts of insecurity in the event they occur. Fixing frequently used files appears to take a shorter span of time when patches are effectively installed and applied, hence enabling prompt detection and containment of security threats. Furthermore, in the case of an event, what IT administrators have is a system that is already fortified with patches that can resolve glitches, which means that they can attend to a problem individually as opposed to attending to a situation while bearing in mind the various other problems that should have been forestalled by the patches.

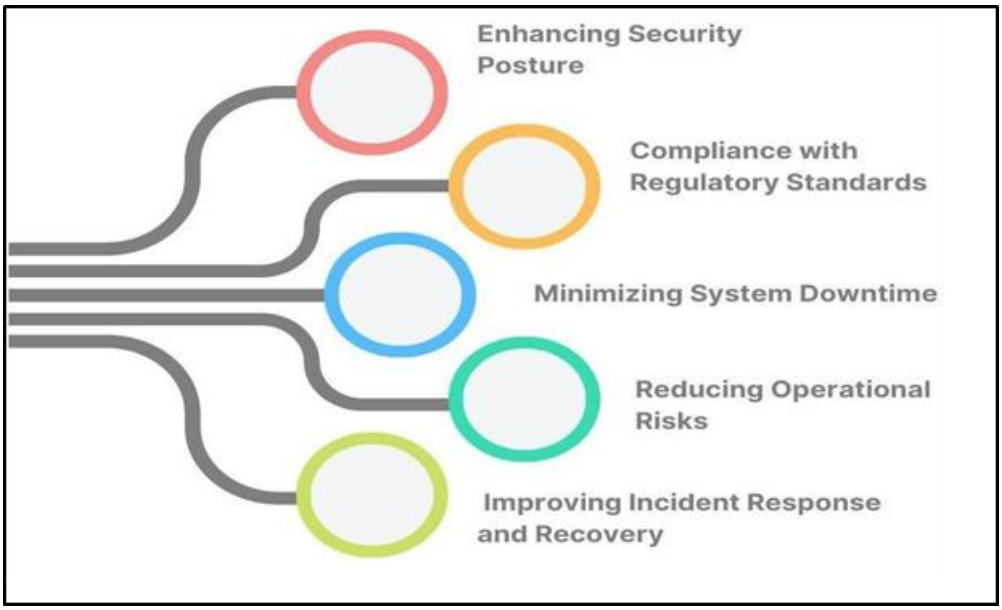

Fig 1. Importance of Patch Management

1.2. Compliance Requirements

- **HIPAA Compliance Requirements (Healthcare)**: The Health Insurance Portability and Accountability Act (HIPAA) sets stringent requirements for the protection of patient data in the healthcare sector. HIPAA mandates several levels of protection that need to be put in place to address the confidentiality, integrity and availability of the PHI. These measures are divided into three groups: administrative, physical, and technical. Administrative safeguards comprise measures aimed at controlling how policies and practices addressing the selection, development,

acquisition, and implementation of security measures are executed. Technical safeguards prevent or limit the technical disclosures of PHI through various means such as technology. Technical safeguards entail the use of technology in the administration of access and also the control of the flow of health information. HIPAA demands frequent updates on systems, for example, security patches increase to ward off any data breach and guarantee the protection of patients' information.

- **FERPA Compliance Requirements (Education)**: FERPA is the act that regulates students' education records within institutions of learning in the United States of America. FERPA entitles the parents or the eligible students the right to access, review, and deny the disclosure of records. It also requires that educational institutions adopt strict measures on access to curb unauthorised persons from accessing student information. Institutions of learning have to keep privacy and security by implementing computer software that can enable only authorised personnel to access the educational records of learners. This is crucial in FERPA regulation compliance since regular patching and security of information systems an important factors of better protection against such flaws, which can let people in a learning institution access the students' information. In this way, educational organisations can protect the students' information and comply with the FERPA requirements when their systems are updated with the latest security patches.

1.3. Ensuring Compliance in Healthcare and Education Sectors

It is important to maintain compliance for healthcare and education institutions to protect sensitive information and avoid the risk associated with it. [5-8] Both of them involve the handling of highly sensitive information and are intertwined with legal requirements such as HIPAA (Health Insurance and Portability Act) for the sector of healthcare sector and FERPA (Family Educational Rights and Privacy Act) for the sector of education sector. HIPAA stipulates that the entities in the healthcare industry must observe administrative, physical and technical measures to achieve the aims of security necessary to safeguard PHI. This involves patching to fix weaknesses in systems that contain such patient information consistently. This also has serious consequences, such as fines, loss of business reputation, but first and foremost, potential violation of patient data. In the same manner, FERPA is imposed in educational institutions, which prohibits any unauthorised individual from accessing students' information.

FERPA lets only those who are allowed to see students' information, depending on their educational records and like HIPAA, needs a timely and secure system upgrade. Specifically, in the sectors used in the research, compliance and automated patch management are imperative in an organisation. Automation can help in the patching process applied in the system since it covers all the critical patches without human interference or delay. Coupled with the ability to monitor these patching requirements in real time, as well as compliance deadlines, audits become much more efficient for an organisation. These make it possible to offer transparent activities with detailed logs and alerts that can easily be produced to demonstrate compliance in case of inspection. It also minimises the risks of the patching that can be turned to gain access to personal details, which, if realised, leads to legal problems. To sum up, from the perspective of compliance in the sphere of healthcare and education, it can be noted that patch management is an effective solution that enables an organization to avoid the majority of failures and problems while satisfying all the legal demands standing for such a field, as well as ensuring the protection of vital information.

2. Literature Survey

2.1. Review of Existing Solutions

Microsoft's WSUS and SCCM are common examples of patch management tools created by Microsoft. WSUS offers centralized approaches to the deployment of Microsoft updates software updates for computers and corporate networks, and it is mostly tailored too small to midsize organizations. [9-12] While WSUS is capable of providing update management for up to ten computers, SCCM enhances the enterprise-level infrastructures with other features such as remote control, software distributing and reporting. However, these tools are mainly only compatible with MS environments and thus do not offer broad compatibility with other systems. Moreover, third- party tools, including ManageEngine Patch Manager Plus, allow organising the work with patches for portable and stationary devices, third-party applications, and using one dashboard. However, they are generally short of contextual knowledge, that is, they are not able to update risk or compliance effects in the same way as the organisation updates its information, which is a major concern in the realm of proactive vulnerability management.

2.2. Gaps Identified

An assessment of current solutions shows that there are three main problems. First,

automation is still primarily centered on partial automations; most frequently, the processes that need manual approvals, setting of schedules, and tracking of remediation jobs. Second, predictive analytics—an essential component for proactive security—is underutilised. None of the ready tools learns the probabilities of vulnerable exploitation and does not prioritise patches based on the current asset importance. Lastly, there is poor or no integration with compliance auditing tools. This separation in turn results in 'silo' working where patch management teams operate entirely separately from compliance officers and this could lead to exposed horn in regulatory reporting and AUD. These weaknesses show the need for smart, automated, and compliance-based patch management solutions.

2.3. Related Work in Healthcare

The challenge to the healthcare sector in patch management is unique due to the nature of the industry and its regulations of the industry. Patching has been viewed as more than a technical activity but as a patient safety issue since about 70% of data breaches in facility surroundings have been caused by unpatched systems. HIPAA has forced healthcare organisations to implement EHRS with integrated patching technologies in place almost by default. But they may not be able to update third-party software or non-clinical systems, therefore leaving system openings that still make the system at risk. He opines that the windows for patching in healthcare IT systems are rather tight and limited; thus, patching is often conducted only after a very long time.

2.4. Related Work in Education

Some of the threats mainly affect K-12 institutions, mainly because of difficulties in affording IT solutions that can cover all their requirements and having a tight staff of IT professionals to help manage these issues. In cases of and many other schools, the organisation lacks a strong IT department or specialised cybersecurity staff, which results in irregular patching or even its complete delay. Secondly, FERPA regulates admission to the records, and data protection measures have never been relaxed in educational institutions. Nevertheless, the access gateways in which these controls rest tend to be the weak link in the armor, thus making the students' private information vulnerable. The progress in distance learning opportunities and Internet connection has added more venues for attacks, meaning that patch management should be both secure and scalable in the case of educational institutions' use.

2.5. Security and Compliance Convergence

While conventional eradication of vulnerability has become insufficient and requires augmentation, particularly in light of compliance. The escalating number of regulations and ever-changing threats mean that organisations can no longer implement patch management as an isolated exercise in compliance. To meet compliance and patch management requirements, these have to be incorporated into patching procedures to ensure that the patches applied are not only addressing the present security vulnerabilities but are aligned with the organisation's compliance standards like HIPAA, FERPA or GDPR. This is very important in producing audit-ready reports, identifying correspondence between the patches and compliance controls to minimise penalties that may result due to non-compliance. Thus, future patch management solutions should be adaptive to policy and should incorporate policy that can be enforced and measured as necessary to support governance needs and visibility.

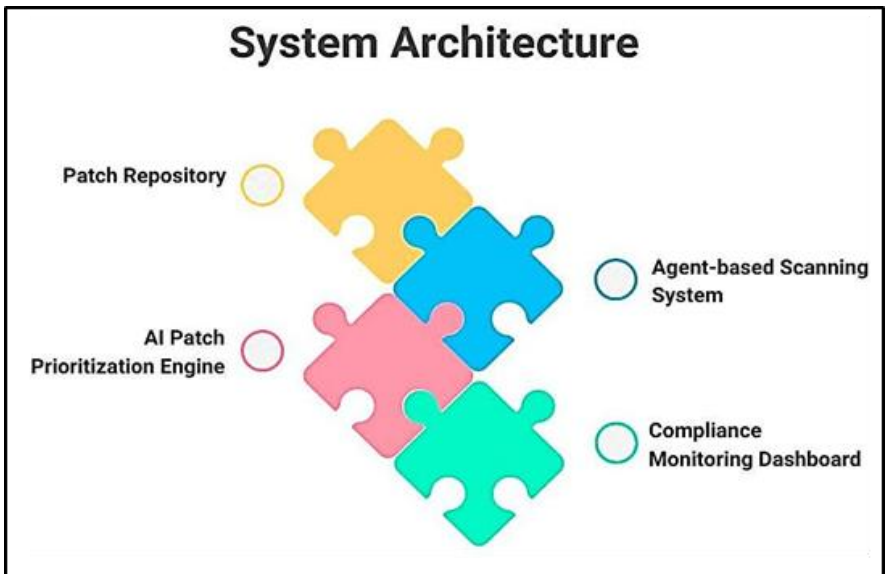

Fig 2. System Architecture

3. Methodology

3.1. System Architecture

The discussed model includes the use of an integrated and smart patch management system that would be technical and compliance-based. [13-16] It comprises four modules, namely the Patch Repository, Agent-based Scanning System, AI Patch Prioritisation component and the

Compliance Monitoring Dashboard.

- **Patch Repository**: This includes Patch Repository, which is the central repository that contains all possible patches, updates and hot fixes. This is done frequently to maintain the updated patch information of the operating system, as well as of any other applications from different vendors. This component of the system plays the role of providing controlled distribution and a rollback capability to be used in case of instability across various enterprises.
- **Agent-based Scanning System**: With support of both the endpoints and servers, the installed Agent-based Scanning System enables precautionary scanning for the absence of patches, changes in the configurations and vulnerability detection. These lightweight agents flood the data to the central server and guarantee visibility of the patching position from the end nodes. This is because the scanning can be done efficiently without consuming the bandwidth, as well as helps manage the remote and distributed infrastructures.
- **AI Patch Prioritisation Engine**: What makes this solution unique is an AI engine that elaborates a patch prioritisation based on risk prodigiously oozes over one hundred scores of continuously progressing machine learning algorithms to detect how many impacts could be observed if certain patches are not applied and to make decisions regarding the deployment of these patches. This implies that the high-risk vulnerabilities are worked on immediately while at the same time avoiding unnecessary downtimes.
- **Compliance Monitoring Dashboard**: Compliance Monitoring Dashboard is used to monitor the compliance and patch deployment details at the administrators' convenience, with real-time status updates. It supports HIPAA, FERPA, and GDPR in mapping patch activity with audit standards. Notifications, paper and visualisation tools make decisions to be made faster and easier, and organisations to be ready for an audit at any time.

3.2. Patch Lifecycle Management

About patch management, it follows cyclic steps to ensure that the vulnerability in a system is effectively managed while minimising the disruption of organization activities. The proposed model adheres to a five-stage process: Discovery, Evaluation, Testing, Deployment, and

Verification.

- **Discovery**: The Discovery phase is an ongoing process of discovering vulnerabilities that come from scanning the organisation's assets and integrating them with sources such as the CVE or Common Vulnerabilities and Exposures database. These are performed by tools that scan the systems against various kinds of security vulnerabilities or misconfigurations, as well as outdated software versions, to come up with an initial list of patches.
- **Evaluation**: During the evaluation phase, all vulnerabilities discerned are rated according to the level of threat they pose to the system. This is done in relation to dependency trees as well as the asset criticality index that assists in outlining how the application of a given patch may impact other elements and services. Another procedure is risk scoring of the vulnerabilities, taking into account the possibility of exploits, their severity measured by the Common Vulnerability Scoring System (CVSS), and impact on business processes.
- **Testing**: Prior to its deployment in production, the chosen patches have to be tested in a simulated environment that brings out all the characteristics of the real setting. Each of these is employed for testing and identifying possible conflict areas, bugs, or inefficiencies that may arise in the development process. This way, the patches can be tested on a sample of the operating system before applying them to live systems, which may cause downtimes.
- **Deployment**: Patched versions are deployed, released at IT endpoints in stages, in what is known as the Deployment phase of clusters. Such an approach divides the program's execution into phases; in this way, IT can track performance and take action if required. Priority is given to high- risk systems, and the remaining low-risk systems are patched later, so that the amount of disruption of services can be kept to a minimum while at the same time the risk exposure can also be controlled.
- **Verification**: Verification is the last process of the software development cycle, and its steps are aimed at confirming that patches have been applied and the OS are operating as required and designed. After the patch has been applied, the scan shows that all the vulnerabilities have been addressed, and logs are reviewed for any signs of error. There are compliance reports whereby, if need arises, roll-back solutions are implemented to negate undesired patches.

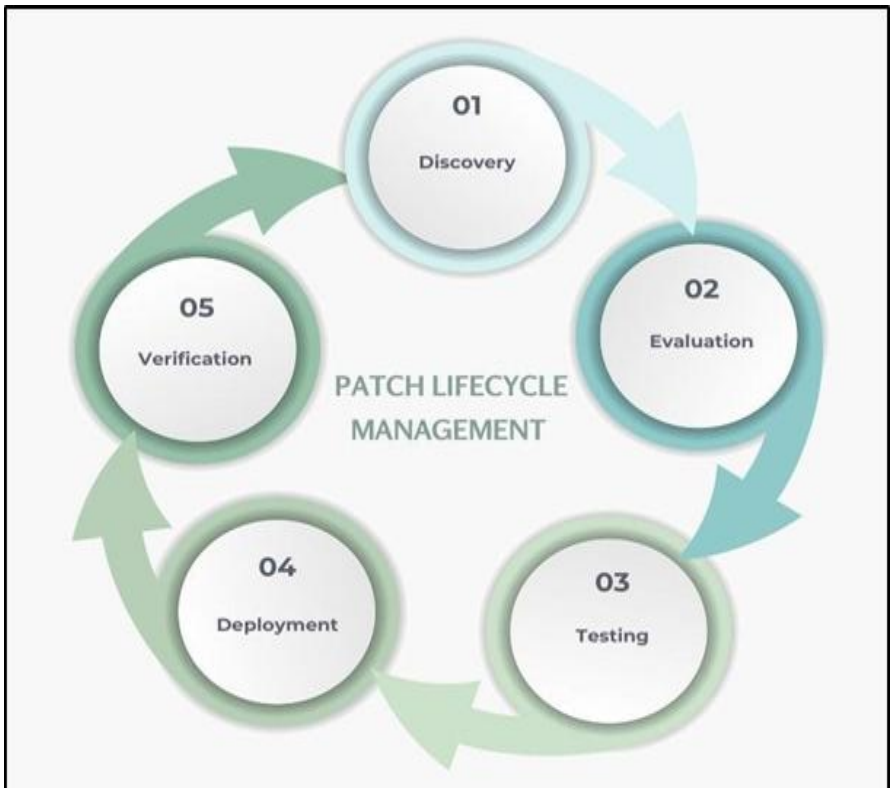

Fig 3. Patch Lifecycle Management

3.3. AI for Patch Prioritisation

The introduction of AI into the patch management process can be highly beneficial as it takes a revolutionary approach of prioritising the vulnerabilities based on risk context. The described approach uses supervised learning algorithms to determine priorities of the patches to be applied to avoid reliance on human decision making and quicker response to potential threats. [17-20] This is especially so since supervised learning informs the model's learning from prior data, where the result of past patching decisions is known, and more prioritisation of new vulnerabilities can, therefore, be accurately made. The sets of structured inputs for the AI engine are acquired from several sources. The measure that has been used is the CVSS score, which is aimed at determining the level of severity posed by the given vulnerabilities. This is, however, not enough, as CVSS does not provide a method for consideration of the environment. Therefore, the model also employs the criticality of assets, which identifies how important the system is within the business, for instance, whether it is managing patient records in a hospital or records of students in an educational facility. Also, in regard to the threat potential, historical exploit data is incorporated to show whether the specific vulnerability has ever been exploited,

thereby giving the model the capability of approximately determining its actual potential in the real world. All these aspects create an overall Priority Index (PI) for each patch by accumulating these elements to form the final value. This index expresses the level of emergency of applying the patch in a way that is a measure of the technical risk, and also the operational impact and probability of the threat. The higher the PI value, the more urgent the patch should be applied, and in the case where the value is relatively low, the patch can be set for some time later and would not affect the program drastically.

This way, the actions of security teams are aligned with the real threats, preliminary testing is not performed actively, and the security of an organisation is improved. The model itself gets better with time, the more data that is fed to it, thus making it an essential component of modern innovative patch management solutions.

3.4. Compliance Module

The Compliance Module is one of the fundamental aspects of the patch management system that governs the security operations within the context of legal requirements and internal policies. These modern days, strict legislation like HIPAA, FERPA, GDPR, and ISO 27001 strictly regulates IT processes, and mere patching is insufficient. They also need to demonstrate to the external auditors that the enterprises' supporting systems remain secure and remain compliant consistently. This is well served by this module, which maps out the patch status of every server and endpoint to an understanding of applicable compliance policies. It has a rule base at the center that maps out the relationship between the system settings and patch levels, and such control sets as dictated by industry standards. For instance, under its Technical Safeguards, HIPAA has a provision on the need to apply security updates promptly, while FERPA mainly embraces access control measures, which rely on patched gateway systems. These regulatory clauses are cross-checked with the actual system state, like missing patches and late, failed updates in the compliance module. This mapping makes it possible to have an eye on compliance with essential standards or the risk of audits during the operations of the system. In addition, the module also has real-time audit trail and reporting features, which help save a lot of time when compliance officers need to prove adequate measures were undertaken during internal or external audits. These logs involve a time stamp, patch number or identification number, identified systems, personnel involved and/or recorded results of any validations, which makes the compliance activities easily traced and auditable. This is

particularly useful in such fields as health and finance, where a lack of compliance attracts penalties and even legal action. In addition to bending patching to the need for compliance monitoring, the system reinforces improved security and also governance, risk management and auditability, limiting operational/legal risks.

4. Results and Discussion

4.1. Experimental Setup

Consequently, to evaluate the effectiveness of the suggested patch management system, a highly elaborate and realistic environment was built in two different areas, healthcare and education. This ensured that each of the sectors had 100 devices and therefore stipulated that there were 200 end-point devices under consideration. Such devices were a combination of business-critical devices, including Windows-based servers, desktops, and Iot devices, which are the standard in both healthcare and education organisations. The experiment was conducted for six months; thus, the patch status, system uptime and overall compliance with industry standards were continually checked for the two devices. The sector involves the healthcare industry, which is controlled by the Health Insurance Portability and Accountability Act, which also indicates that security and confidentiality should be met strictly, especially in areas requiring timely patching to protect important data regarding patients. As for the education sector, the Family Educational Rights and Privacy Act (FERPA) was designed to enforce strict measures of controlling access to the students' data. During the course, devices in each sector were connected to the patch management system, which involved in the role of the monitoring of the installation of security patches, the assessment of the overall vulnerability status of the system, as well as the checking of compliance with the established regulatory measures. It was a strategy to monitor the success of the approach of reducing patching time, raising compliance levels and lowering downtime while covering the specifications of the healthcare and educational sectors. To that end, the experiment sought to determine patch management's applicability and ability to provide worthwhile results under the known regulatory and operational differences between the two sectors.

4.2. Key Metrics Evaluated

The assessment of the proposed model was done based on the following performance indicators:

- **Patch Time**: This is the aggregate time in which patching activities involve assessing the environment, identifying the patch, deploying it and implementing it onto the systems in the environment. This is important in helping ascertain the time taken to address vulnerabilities, thus reducing the time that is taken to get off a network, system or device, and some of the risky threats that may be faced. The need for faster patch times is even higher if you are in such an environment as healthcare or an educational institution, where a delay in patching can lead to an increase in the security threat level or non- compliance with existing legislation. In the proposed system, the effectiveness of automation and AI to prioritise and bring patching frequency, critical vulnerabilities are prioritised and deployed for protection as and when required for all the endpoints.
- **Compliance Score**: The Compliance score depicts the level of conformity within the experiment setup in regards to the regulatory patching policies and procedures applicable to each industry. For instance, in the healthcare sector, it would meet requirements from the Health Insurance Portability and Accountability Act, which concerns frequent patching of medical and IT equipment and systems, or in the education sector, to conform to the Family Educational Rights and Privacy Act or FERPA, on data protection. This metric is very useful in making certain that the organisation is in compliance with the law and is not paying fines for noncompliance. These include the compliance re- enabling tools that enable the tracking of the status of the patches in real time, to enhance the use of reports on the compliance status, as well as preparedness for audits.
- **Downtime Impact**: Downtime Impact quantifies the decrease in time that is lost due to more instances of random events that may occur at the time of the patch on VP. Patches, which enhance the security of an organisation's systems and networks, can become a thorn in the flesh since they may cause outages or slow down the system's performance when they are not well tested, certified, or rolled out. Here, reducing downtime is of high essence, and this is more so in industries such as the health sector, where the system adopted acts as a critical tool in patient treatment. There was a benchmarking test on how the system was able to install patches without compromising the users' operations. In this model, the system attempted to follow a pilot implementation strategy where patch application was gradual so that, in case

something went wrong, there would not be an interruption of service.

4.3. Performance Analysis

This has proved that the use of priority and automated patch deployment has a positive impact on patch management practices in both the areas of health care and education. The proactive alerts will be offered by the system, leveraging rules-based machine learning frameworks to prioritise the patches based on the level of threat by vulnerability, criticality of the assets, and the real-time threats. This way, the amount of time spent in the identification, analysis, and deployment of the patch is optimum, and the organisations can respond to the risks much more effectively and in a lesser time.

Table 1: Percentage Reduction in Avg. Patch Time

Sector	Avg. Patch Time Reduction (%)
Healthcare	75%
Education	73.33%

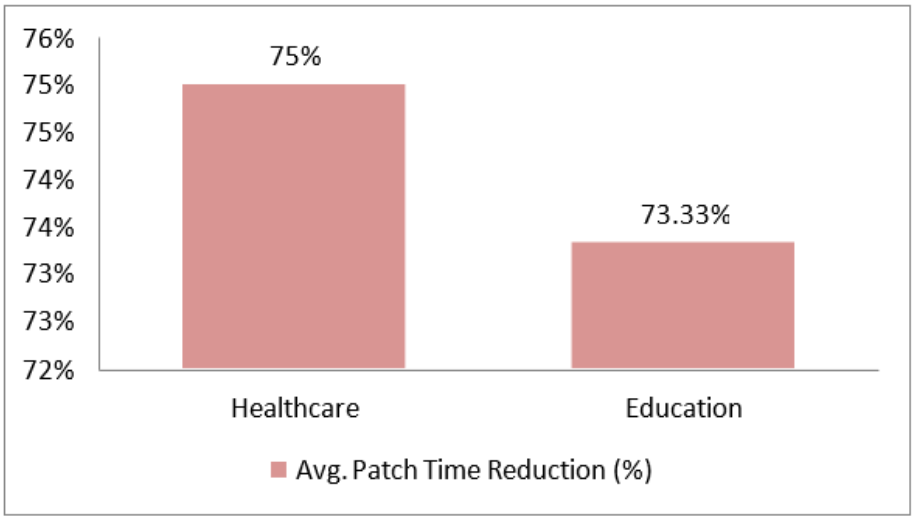

Fig 4. Graph representing Percentage Reduction in Average. Patch Time

- **Healthcare Sector**: Regarding the application of smart patching in the healthcare field, the enhancement achieved an impressive 75% cut in mean patch time. The healthcare sector is not only vital for patients' lives, and, as such, the continuity of the processes is significant, but it also deals with sensitive patient information. The priority was based on the risk and the severity of the weakness in question, which allowed focusing on high-pressure threats, reducing the risk of an attack. Asset

importance was also an aspect recognised by the AI system, meaning that in critical systems, patches can be rolled out. The response was a shorter time for patch and certainly, the improved system security to ensure compliance with the highest standard as required by HIPAA.

- **Education Sector**: Likewise, under the business management domain, patching frequency was reduced by 73.33% due to the implementation of automated patch deployment as well as the use of IA for prioritisation. Automating patching is also beneficial for educational institutions that usually have a limited budget and workforce, hoping its efficiencies help IT teams to attend to other priorities. To sum up, the application of automation to patch deployment and a proactive AI approach to analyse the probability of the specific application exploits and system criticality allowed the education sector to decrease patch times. This enhancement not only enhances security, which is paramount for any firm, but also guarantees that FERPA and other data protection laws are not violated.

4.4. Compliance Improvement

Table 2: Compliance Score Comparison

Sector	Before (%)	After (%)
Healthcare	67%	91%
Education	59%	87%

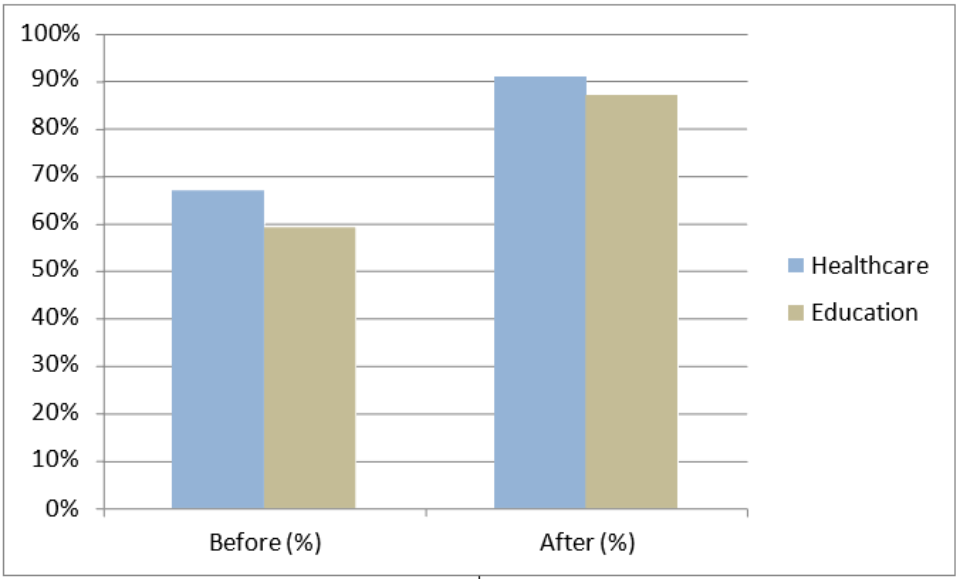

Fig 5. Graph representing Compliance Score Comparison

The integration of the compliance module within the patch management system had the effect of enhancing compliance scores within both sectors. The system could map out regulatory patching, such as HIPAA for medical institutions and FERPA for educational institutions, to compare their compliance in real-time systems for constant feedback. In this regard, before the implementation of the system, it was noted that the compliance level in the healthcare sector was at sixty seven percent while that of the education sector was at fifty nine percent. It was not until the system and its features that enhanced the score to 91 % for health care and 87% for education were deployed. This means a significant improvement in the capacity of both sectors. These enhancements were accomplished through the use of the compliance module, especially in the areas of monitoring and auditing in real time. This was based on the track of patch statuses with regard to the instructed regulatory requirements, to track any failure in compliance. For example, in case of missed or delayed patch deployment on a machine, the system was to notify the administrator and provide information to address the problem immediately. By practicing this kind of strategic measure, compliance breaches were prevented, and fewer alterations were susceptible to security breaches due to delayed patching and missed security updates. In addition, the compliance module produced comprehensive audit trails that were useful for investigative purposes, such as compliance inspection or audit. These logs provided clear documentation of the patching process, ranging from which patches were installed, when they were installed, and by whom. Not only did this enhance the visibility of the processes related to patch management, but it also diminished the time spent preparing for the audit, as well as the time needed to prove compliance. Thus, there were enhanced mechanisms of compliance with health and education standards, increased operational efficiency and a reduction in compliance-related risks.

4.5. Discussion

The patch prioritisation engine that was developed by incorporating new artificial intelligence features made it easier to manage patches and minimise the accumulation of patches that were yet to be implemented, especially for both the healthcare and education units. Due to the use of the algorithms, the system was able to sort through all the vulnerabilities and present the most severe ones to the IT team for resolution. This method of intelligent patch prioritisation has thus resulted in a huge improvement of the average patch time, which is now close to 70%, in both sectors. It also increased the overall efficiency of the system’s protection

and guaranteed that certain risks that could be exploited by intruders were addressed before they occurred, hence minimising the number of breaks or downtimes. Regarding compliance, the use of compliance dashboards assists in achieving greater compliance since it is part of the measures taken to enhance compliance. These dashboards helped the administrators to keep track of whether the related systems for compliance are up to date in real-time and also identify commonalities and crucial points of non-compliance. This ethnicity made organisations respond to issues before they become complex, and it furthermore helped improve the compliance with healthcare laws by 24% and education laws by 28%. By proactively addressing compliance, enterprises are able to process it more appropriately to meet the requirements of regulations like HIPAA in healthcare and FERPA in education. Moreover, it is noteworthy to mention that the ability to have real-time audit logs and role-based access to the system enhances objectivity and security. These features were of key importance to the organisation since they helped them to provide auditors with a detailed audit trail that included MAC address and other data, which are vital during regulatory body inspections and also helped in tightening up on security since only privileged users were able to input data into patch management systems. Such automation was evidenced by the fact that the auditors were able to cut 50% manual effort involved in the preparation of the audit while at the same time enhancing other related operations to improve the organisational operations. All in all, the results prove that the proposed patch management system is indeed useful in promoting the enhancement of overall cybersecurity while at the same time preparing an organisation for an audit exercise to ascertain its compliance without compromise on security.

5. Conclusion

In the modern environment, when the world is connected and sensitive information is in high demand, the automation of the patch management process as part of cybersecurity has become compulsory, especially in healthcare and educational institutions. This work shows that artificial intelligence automates various measures to enhance both endpoint protection as well as compliance with the rules. Generally, manual and conventional patch management are known to be time-consuming and prone to errors, which extend the system downtime, and increase vulnerability exposure and non-compliance. Using AI techniques in patching, this system helps organisations intelligently select the critical patches and subsequently apply them, reducing the time and also minimising vulnerabilities.

This shift is not only advantageous in enhancing the firm's cybersecurity measures, but it also fulfils regulatory guidelines like the HIPAA and FERPA regulations on timely and properly documented patching. Throughout this investigation, the outcomes demonstrated that it was possible to significantly increase both the speed of patch deployment as well as the compliance levels and organisational efficiency with the help of an AI-based patch management system. These advancements were invaluable, especially in fields that demand high safety measures for patients' information in healthcare and students' information in education. Compliance scores increased, which proved the capability of the system in adhering to the regulatory standards of the organisations and offering them with timely solution to their security situation. Additionally, reporting and audit trails that have been automated helped alleviate the load from compliance audits, which helped IT concentrate on the preventive measures and improvements of the systems.

Thus, the necessary further developments of automated patch management systems are presented below: This is why new and valuable opportunities are being sought to integrate decentralised blockchain-based audit trail solutions. Blockchain technology can offer an architected and more comprehensive solution to demonstrate patching change and history in a way that is segregated and extraordinarily difficult to alter, which will be particularly useful for compliance-oriented domains. Further, the federated learning models could be pursued to implement predictive patching. This way, federated learning could improve the AI algorithms with data from several organizations and organisations without sharing the sensitive information, which could help better decision- making of the patching solutions based on the global threat level.

This paper shows that there is promise in using AI for automating the patch management process. In the current world, the level of cybersecurity threats is constantly rising and hence calls for measures such as these systems to expedite compliance with increasing standards in the protection of data. This paper shows how the underlying concept of patch management in high-risk sectors is the utilisation of automation and the value of AI.

References

[1] Boda, V. V. R., &Immaneni, J. (2023). Automating Security in Healthcare: What Every IT Team Needs to Know. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 4(2), 46-56.

[2] von Stockhausen, H. M., & Rose, M. (2020, March). Continuous security patch delivery and risk management for medical devices. In 2020 IEEE International Conference on Software Architecture Companion (ICSA-C) (pp. 204-209). IEEE.

[3] Wu, R., Ahn, G. J., & Hu, H. (2012, January). Towards HIPAA-compliant healthcare systems. In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (pp. 593-602).

[4] Chen, J. Q., &Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. International Journal of Healthcare Management, 10(2), 135-146.

[5] Achieving Continuous Compliance with Automated Patch Management, jetpatch, online. https://jetpatch.com/blog/patch- management/automated-patch-management-for- continuous-compliance/

[6] Kovalenko, M., Rusnak, A., &Lomonosov, D. (2021). Ways of ensuring the compliance of the activities of higher education institutions with modern challenges. Baltic Journal of Economic Studies, 7(5), 104-113.

[7] Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, 20(1), 44-51.

[8] Cairns, A., &Yarker, Y. E. (2008). The role of healthcare communications agencies in maintaining compliance when working with the pharmaceutical industry and healthcare professionals. Current medical research and opinion, 24(5), 1371-1378.

[9] Dissanayake, N., Zahedi, M., Jayatilaka, A., & Babar, M. A. (2022). Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. Proceedings of the ACM on Human-computer Interaction, 6(CSCW2), 1-29.

[10] Yadav, G., Gauravaram, P., Jindal, A. K., & Paul, K. (2022). SmartPatch: A patch prioritisation framework. Computers in Industry, 137, 103595.

[11] Gerace, T., &Cavusoglu, H. (2009). The critical elements of the patch management process. Communications of the ACM, 52(8), 117-121.

[12] AhmadiMehri, V., Arlos, P., &Casalicchio, E. (2022). Automated context-aware vulnerability risk management for patch prioritisation. Electronics, 11(21), 3580.

[13] Zhu, X., Healey, R. G., &Aspinall, R. J. (1998). A knowledge-based systems approach to the design of spatial decision support systems for environmental management. Environmental management, 22(1), 35-48.

[14] Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management systematic literature review of challenges, approaches, tools and practices. Information and Software Technology, 144, 106771.

[15] Yoon, S., Yoon, H., Zahed, M. A., Park, C., Kim, D., & Park, J. Y. (2022). Multifunctional hybrid skin patch for wearable smart healthcare applications. Biosensors and Bioelectronics, 196, 113685.

[16] Wu, T., Wu, F., Qiu, C., Redouté, J. M., &Yuce, M.R. (2020). A rigid-flex wearable health monitoring sensor patch for Iot-connected healthcare applications. IEEE Internet of Things Journal, 7(8), 6932-6945.

[17] Gunn, P. P., Fremont, A. M., Bottrell, M., Shugarman, L. R., Galegher, J., &Bikson, T. (2004). The health insurance portability and accountability act privacy rule: a practical guide for researchers. Medical care, 42(4), 321-327.

[18] Automated Patching & Endpoint Management, srccybersolutions, online. https://srccybersolutions.com/solution/automated- patching

[19] Goel, S., Kiran, R., &Garg, D. (2012). Vulnerability management for an enterprise resource planning system. arXiv preprint arXiv:1209.6484.

[20] Saffady, W. (2020). Managing information risks: threats, vulnerabilities, and responses. Rowman& Littlefield.