Autonomic Computing in Smart Buildings: Challenges, Opportunities, and Future Perspectives

1st Mohsen Rahimi
HKUSpace
Hong Kong
20212303@learner.hkuspace.hku.hk

2nd Dr. Yeung Lam
HKUSpace
Hong Kong
eelyeung@gmail.com

***Index Terms*—Autonomic, Smart, Building, IOT, AI, ML**

I. Introduction

The rapid growth of urbanisation and advancements in digital technologies have led to the emergence of smart buildings as a critical component of modern cities. Smart buildings incorporate advanced automation, monitoring, and control systems to optimise energy consumption, enhance occupant comfort, and improve overall building performance [1]. Autonomic computing (AC) is a promising approach that can contribute significantly to the efficient management and operation of smart buildings. AC refers to the development of self-managing computing systems that can adapt, optimise, and recover from failures with minimal human intervention. By leveraging the principles of autonomic computing, smart buildings can become more intelligent, responsive, and adaptable to changing conditions and user needs [2].

The goal of this research is to investigate the application of autonomic computing in the field of smart buildings, review the current state of the art, identify limitations and challenges, and design an autonomic solution as a proof of concept. This paper will also explore the potential ethical implications of implementing autonomic computing in smart buildings and provide insights into future trends and developments in this area. Through a comprehensive analysis and evaluation of information from various sources, this research aims to contribute to the ongoing discourse on the role of autonomic computing in shaping the future of smart buildings and sustainable urban environments and in particular security in smart buildings

In the following sections, we will delve deeper into the literature on autonomic computing and its application in smart buildings, discuss the current state of the art, analyse real-world examples and current trends, and propose a proof of concept for an autonomic solution addressing the identified challenges. Finally, we will examine the ethical considerations and future predictions for autonomic computing in smart buildings.

II. Literature Review

Autonomic computing (AC) is a computing paradigm inspired by the human autonomic nervous system, which aims to develop self-managing computing systems capable of self-configuration, self-optimisation, self-healing, and self-protection. AC has been widely researched and applied in various fields, including smart buildings, where it can significantly enhance their efficiency, sustainability, and occupant satisfaction [2].

A. Autonomic Computing in Smart Buildings

In recent years, the application of autonomic computing in smart buildings has gained considerable attention from researchers and industry practitioners. The integration of AC principles into smart building management systems enables these buildings to adapt, optimise, and recover from failures with minimal human intervention, thereby improving overall performance and reducing operational costs.

B. Current State of the Art

Several studies have explored the implementation of autonomic computing in smart building systems, focusing on aspects such as energy management, fault detection and diagnosis, and occupant comfort optimisation [3]. These studies have proposed various algorithms, architectures, and frameworks that leverage machine learning, artificial intelligence, and data analytics techniques to enable smart buildings to operate autonomously [4].

C. stakeholders

Key stakeholders in the application of autonomic computing to smart buildings include building owners and operators, technology providers, architects and engineers, occupants, and policymakers. These stakeholders play a crucial role in driving the adoption and integration of AC solutions in smart buildings, ensuring their successful implementation and widespread acceptance [5].

D. Applications and Benefits

Autonomic computing has numerous applications in smart buildings, including:

- Energy management: By using AC algorithms, smart buildings can optimise energy consumption by autonomously adjusting HVAC, lighting, and other building systems based on occupancy patterns and external conditions [6].
- Fault detection and diagnosis: AC-based systems can automatically identify and diagnose faults in building

equipment, enabling proactive maintenance and reducing downtime [2].
- Occupant comfort optimisation: Autonomic computing can be used to personalise indoor environments based on individual preferences and needs, thus enhancing occupant satisfaction and well-being [7].

E. History of Autonomic Computing in Smart Buildings

The concept of autonomic computing was first introduced by IBM in the early 2000s [8]as a vision for self-managing computing systems. IBM engineers saw the need to develop smart systems that could monitor, repair and manage themselves to a high degree. In 2004, IBM Press published the 336-page "Autonomic Computing" book that described systems that "install, heal, protect themselves, and adapt to your needs – automatically." Since then, AC has evolved and expanded into various domains, including smart buildings. Early research in this area focused on developing basic frameworks and algorithms for autonomic control of building systems. Over the years, advances in sensor technology, data analytics, and artificial intelligence have paved the way for more sophisticated and comprehensive AC solutions for smart buildings, enabling them to achieve higher levels of autonomy and intelligence [9].

One of the earliest examples of autonomic computing in smart buildings is the B-SMART reference architecture, which accelerates the application of artificial intelligence in smart buildings. B-SMART supports both startup and ongoing commissioning, and it supports autonomic smart building operations [10].

III. Restrictions and Challenges with Real-World Examples

While the literature review highlights the potential benefits of applying autonomic computing to smart buildings, there are certain restrictions and challenges that need to be addressed to ensure successful implementation [11]. This section will discuss these challenges and provide real-world examples to illustrate their impact on the adoption and integration of autonomic computing in smart buildings.

A. Security and privacy concerns

One of the issues with smart technology is that they are heterogeneous (different architectures in terms of hardware and software). There is not a standardisation for the IoT environment. Even though the most familiar communication protocol used is Bluetooth, the messaging protocol system is different. Fig 1 is a table that shows a comparison between messaging protocols used in IoT systems [12], which causes concerns in terms of security and privacy [13]. It is paramount to consider the fact that smart home devices are battery-driven and might use low-power CPUs, including lower clock rates and small throughput [14]. In [11] , the authors performed security tests on a sensor with 8 MHz of CPU frequency, 10 KB of RAM memory and 48 KB of program memory, which proved that applying security mechanisms are not feasible in small IoT devices. For instance, public key algorithms such as RSA and ECC [15] are very intensive for computational processing on micro controllers and requires many instructions to perform one security process. Therefore, tactics, techniques and procedures (TTPs) executed by malicious attackers are being developed with nefarious purposes, making more challenging the protection of home networks. A smart device can be physically accessible making them prone to tampering attacks to reduce billing costs. An example is a case published in Wired [16]where hackers can use lasers to "talk" to your amazon echo or google home, including a demonstration.

Increased adoption of smart devices has seen an increase in cyber threats by the execution of multiple procedures in order to leak or tamper information as well as the disruption of services. Some risks are mentioned below.

- Eavesdropping Attack: Also called sniffing, consists about gathering real time information that smart devices, micro controllers and smartphones transfer through a network. It can allow attackers to intercept user privacy and break data confidentiality without disturbing the transmission. In a smart home network, an eavesdrop attack can be used to steal login/password credentials when a user authenticates to the smart home app which could allow hackers to take control of the smart home environment [17].
- Malicious Code Injection: Malicious codes are normally scripts (software programmed), which can be inserted into the smart home app, allowing attackers to exploit vulnerabilities including authentication bypassing which allows access to unauthorised entities. In smart home environments, code injection threats present an impact on user's privacy and confidentiality including the capability of attackers to access the system, including harmful operations like stealing personal data [18].
- Man-in-the-Middle (MitM) Attack: An attacker can impersonate a legitimate device within the network which can steal, insert, modify or drop packets. According to [19].
- Attacks against Home Monitoring and Control: Some threats can include an attacker performing a message tampering or replay attack. For example, the attacker can imitate the client's cloud service sending a message to the ESI requesting to turn off all the devices connected to the home network because they were increasing the electricity bill [20]. In case of message tampering or replay attack, the attacker could send a signal to a smart washing machine to repeatedly wash the clothes or increase the temperature of the oven from 120°C to 240°C. Other risks are mentioned below:
- Man-In-The-Browser (MitB) Attack [21].
- Denial of Service (DoS) Attack [22].

B. Implementation complexity

Smart buildings are constantly evolving and subject to continuous change as new devices are added, removed or updated. One of the most important aspects is connectivity with other devices, where robust connectivity is the key to predictable

system behavior. In addition, the design and implementation of autonomic computing solutions can be complex due to the need to integrate various sensors, actuators, control systems, and communication protocols. This complexity may result in higher development costs and longer deployment times [23].

C. Interoperability

Smart buildings often consist of diverse systems and components from different manufacturers, which may not be easily compatible with each other . This lack of interoperability can hinder the seamless integration of autonomic computing solutions, limiting their effectiveness and scalability [24].

D. High initial investment

Deploying autonomic computing solutions in smart buildings may require significant upfront investment in hardware [23], software, and infrastructure upgrades, which can be a barrier for some building owners and operators.

IV. Current Trends

while there are several restrictions and challenges in applying autonomic computing to smart buildings, ongoing research and industry trends show promise in overcoming these obstacles and unlocking the full potential of autonomic computing in enhancing smart building performance and occupant satisfaction [25].

A. Standardisation and open-source platforms

To address interoperability challenges, industry stakeholders are working on developing standardised communication protocols and open-source platforms that enable seamless integration of diverse systems and components [26].

B. Advanced data analytics and AI techniques

The ongoing advancements in data analytics and artificial intelligence are enabling the development of more sophisticated and robust autonomic computing algorithms, which can better adapt to complex building environments and occupant needs. AI techniques have the potential to analyse large data sets faster than a human operator. The data is presented for interpretation, showing trends and possible suggestions in order to improve the performance of the programmed services. There is an extended literature review of the application of AI in smart homes presented in [18], categorised in five clusters which are data processing, decision-making, voice recognition, activity recognition and prediction making.

C. Cybersecurity measures

Researchers and industry practitioners are increasingly focusing on addressing security concerns by designing autonomic computing solutions with built-in cybersecurity measures [27] and data protection mechanisms.

V. Proof of Concept - Autonomic Solution Design

The Adaptive Smart Building Management System (ASBMS) is an autonomic solution designed to address the identified restrictions and challenges in applying autonomic computing to smart buildings. This proof of concept aims to create a flexible, secure, and scalable solution for smart buildings that seamlessly integrates with diverse systems and components while optimizing energy consumption, enhancing occupant comfort, and reducing operational costs. The ASBMS leverages the principles of autonomic computing to achieve self-management in smart buildings by using the potential of AI, specifically Deep Learning and Machine Learning.

The ASBMS consists of the following key components and Principles :

A. Sensor and Actuator Network:

A network of IoT-enabled sensors and actuators, strategically placed throughout the building [28], collects real-time data on various parameters such as temperature, humidity, occupancy, and energy consumption. The actuators control HVAC, lighting, and other building systems based on the decisions made by the autonomic controller.

B. Data Management and Processing Layer:

This component collects, stores, and processes the data from the sensor network, ensuring data integrity and security. It employs advanced data analytics and machine learning algorithms to extract valuable insights and patterns from the data, which feed into the autonomic controller [29].

C. Autonomic Controller:

The core of the ASBMS, the autonomic controller, uses AI-based algorithms to make intelligent decisions based on the processed data. It continuously monitors the building's performance and dynamically adjusts the control strategies for various systems to optimise energy consumption, ensure occupant comfort, and maintain system reliability [24].

D. User Interface:

A user-friendly interface allows building occupants and operators to interact with the ASBMS, customise settings, and monitor building performance. The interface also provides notifications and alerts in case of system anomalies, maintenance requirements, or potential security threats [30].

E. Security and Privacy Module:

This module ensures the protection of sensitive data and the building's systems from potential cyberattacks and privacy breaches by implementing robust encryption, authentication, and access control mechanisms [31].

VI. Proof of Concept - 4 Autonomic Computing principles for Self-Management in Smart Buildings

The ASBMS achieves self-management in smart buildings through the following autonomic computing principles [32]:

A. Self-configuration

Self-configuration refers to the ability of a system to automatically set up and configure its components without human intervention. In smart buildings, self-configuration can be applied to various systems during the initial setup, maintenance, or when adding new components to the building [32].

Here are some real-world examples of self-configuration in smart buildings:

- Plug-and-play devices: In a smart building, devices such as sensors, actuators, and controllers can be designed to be plug-and-play, meaning they can automatically configure themselves when connected to the building's network. This simplifies the installation process and reduces the need for manual configuration. For example, when a new sensor is added to the building's HVAC system, it can automatically detect its location, calibrate itself, and start sending data to the central control system without any human intervention [30].
- Automatic network configuration: Self-configuration can be applied to the building's network infrastructure, allowing it to automatically detect and configure new devices, assign IP addresses, and manage communication protocols. This simplifies network management and ensures seamless integration of new components [3].
- Self-configuring security systems: In a smart building, the security system can automatically configure itself based on the building's layout and the location of doors, windows, and other access points. For example, when a new security camera is installed, it can automatically adjust its field of view and resolution to cover the desired area, and configure its motion detection settings to minimize false alarms [27].

B. Self-optimisation

By continuously analysing real-time data and using AI-based algorithms, the ASBMS identifies opportunities for energy savings and performance improvements, adjusting system settings to achieve optimal efficiency and occupant comfort. In smart buildings, self-optimization can be applied to various systems, such as HVAC, lighting, security, and energy management. Here are some real-world examples of self-optimization in smart buildings [32]:

- Adaptive HVAC systems: In a smart building, the HVAC system can optimize its performance based on factors like occupancy, outdoor temperature, and time of day. For example, the system can automatically adjust the temperature and airflow in different zones of the building based on the number of occupants and their preferences. This not only improves comfort but also reduces energy consumption. The ABB Ability™ Smart Sensor [33] for HVAC is an example of a solution that enables self-optimization by monitoring and analyzing data from HVAC equipment [6].
- Intelligent lighting systems: Smart lighting systems can optimize their performance by adjusting the intensity and color temperature of the lights based on the time of day, occupancy, and available natural light. For example, the system can automatically dim the lights when there is sufficient daylight or turn off the lights in unoccupied areas. This helps in reducing energy consumption and enhancing the occupants' well-being. Philips' Interact Office is an example of a smart lighting system that optimizes energy usage and enhances employee productivity [6].
- Security and access control: In a smart building, the security system can optimize its performance by analyzing data from various sensors and cameras to detect potential threats and respond accordingly. For example, the system can automatically adjust the sensitivity of motion detectors or the resolution of security cameras based on the level of activity in a specific area. This ensures a secure environment while minimizing false alarms and reducing energy consumption. Honeywell's Pro-Watch® Integrated Security Suite is an example of a solution that optimizes security operations in smart buildings [30].
- Energy management: Smart buildings can optimize their energy consumption patterns based on real-time data from sensors and external sources like weather forecasts and energy prices. For example, the building can automatically switch to renewable energy sources when they are available or adjust the HVAC system's operation to minimize energy consumption during peak demand periods. This helps in optimizing energy usage and reducing costs. Schneider Electric's EcoStruxure™ [34]Building is an example of a platform that enables self-optimization of energy management in smart buildings.

C. Self-healing

Self-healing in smart buildings refers to the ability of a building's systems to autonomously detect, diagnose, and repair faults or malfunctions without human intervention. This capability enhances the building's reliability, reduces downtime, and minimizes maintenance costs [2].

In ASBMS, self-healing can be applied to various systems, such as HVAC, lighting, security, and energy management. Here are some examples of self-healing in smart buildings:

- Fault detection and diagnostics: Smart buildings can use sensors, IoT devices, and data analytics to continuously monitor the performance of various systems and detect anomalies or faults. For example, an HVAC system can monitor the temperature, humidity, and airflow in different zones of the building and compare them with expected values. If a discrepancy is detected, the system can automatically diagnose the issue, such as a malfunctioning sensor or a blocked air filter, and take corrective action [27].
- Redundancy and fail over: Smart buildings can incorporate redundancy and fail over mechanisms to ensure continuous operation in case of a component failure. For example, if a critical sensor or controller in the

HVAC system fails, the system can automatically switch to a backup device or use data from other sensors to maintain optimal performance. This minimises downtime and ensures the building's systems continue to operate efficiently [24].
- Predictive maintenance: Self-healing smart buildings can use data analytics and machine learning algorithms to predict when a component is likely to fail and schedule maintenance before the failure occurs. This proactive approach reduces the risk of unexpected failures, minimises downtime, and extends the lifespan of the building's systems [35].
- Automatic software updates and patches: Smart buildings can automatically update their software and firmware to fix bugs, vulnerabilities, or performance issues. This ensures that the building's systems are always up-to-date and reduces the risk of security breaches or system failures due to outdated software [31].
- Self-healing concrete: Building scientists are exploring innovative ways to enhance the durability and longevity of infrastructure by incorporating self-healing properties into construction materials. One such approach involves the use of bacteria in concrete formulations. These bacteria, typically from the Bacillus family, are encapsulated in microcapsules or mixed with nutrients and embedded within the concrete matrix. When micro-cracks form in the concrete, the bacteria are exposed to moisture, which activates them and triggers the production of calcium carbonate. The calcium carbonate then fills the micro-cracks, effectively healing the concrete and preventing further damage [36].

D. Self-protection

Self-protection in smart buildings refers to the ability of a building's systems to autonomously detect, prevent, and respond to potential threats or hazards, ensuring the safety and security of the building and its occupants. This capability enhances the building's resilience, minimizes the risk of damage or loss, and reduces the need for manual monitoring and intervention [32].

In ASBMS, self-protection can be applied to various systems, such as security, fire safety, and structural health monitoring. Here are some examples:

- Intrusion detection and prevention: Smart buildings can use sensors, cameras, and data analytics to continuously monitor the building's perimeter and interior for potential security threats, such as unauthorized access or suspicious activity. If a threat is detected, the system can automatically take preventive measures, such as locking doors, activating alarms, or notifying security personnel [27].
- Fire detection and suppression: Smart buildings can use advanced sensors and IoT devices to detect the early signs of a fire, such as smoke, heat, or gas leaks. If a fire is detected, the system can automatically activate fire suppression measures, such as sprinklers or gas-based extinguishing systems, and alert the occupants and emergency services [31].
- Structural health monitoring: Smart buildings can use sensors and data analytics to continuously monitor the building's structural health, such as vibrations, deformations, or cracks. If a potential issue is detected, the system can automatically alert the building's management and maintenance teams, allowing them to take preventive measures and avoid potential damage or collapse [37].
- Cybersecurity: Smart buildings can use advanced cybersecurity measures, such as encryption, firewalls, and intrusion detection systems, to protect the building's network and data from potential cyber threats. If a cyber threat is detected, the system can automatically take preventive measures, such as blocking the attacker's IP address, isolating affected devices, or updating the software to fix vulnerabilities [27].
- Environmental monitoring and response: Smart buildings can use sensors and data analytics to monitor the building's environment for potential hazards, such as air pollution, water leaks, or extreme weather conditions. If a hazard is detected, the system can automatically take preventive measures, such as adjusting the HVAC system to maintain indoor air quality, shutting off water valves to prevent flooding, or activating backup power systems during a power outage [38].

Some of the real-world example of a smart building or platforms are Desigo CC building management platform [39], IBM Watson IoT Center in Munich [40]and The Edge in Amsterdam [41], This building, designed by PLP Architecture [42] and developed by OVG Real Estate, is considered one of the greenest and most intelligent buildings globally.

In general by incorporating these autonomic computing principles, the ASBMS proof of concept demonstrates a feasible solution for enhancing the performance, efficiency, and occupant satisfaction of smart buildings while addressing the identified challenges and restrictions.

VII. Future Predictions

As the field of autonomic computing continues to evolve and smart buildings become increasingly prevalent, we can anticipate several developments and advancements in the integration of autonomic computing in smart buildings over the next few years. This section discusses potential trends, opportunities, and challenges that may shape the future landscape of autonomic computing in smart buildings [23].

A. Integration of advanced AI and machine learning techniques

As AI and machine learning technologies continue to advance, we can expect more sophisticated algorithms and models to be integrated into autonomic computing solutions, enabling better decision-making, prediction, and adaptation capabilities for smart buildings [35].

B. Proliferation of IOT devices and sensors

The ongoing growth in the adoption of IOT devices and sensors will contribute to richer, more accurate data collection, enhancing the effectiveness and responsiveness of autonomic computing solutions in smart buildings [30].

C. Edge computing and 5G connectivity

The deployment of edge computing and 5G networks will enable faster data processing and communication, resulting in more efficient and real-time decision-making for autonomic smart building systems [43].

D. Digital twin technology

The digital twin of a smart home is defined as: using a priory information (e.g., architectural plans, input from inhabitants) and given input sensory data (e.g., home automation and robot sensors), build a continuous model including robots and user models. The integration of digital twin technology with autonomic computing solutions can provide virtual simulations and testing environments for smart buildings, allowing for improved building design, performance optimisation, and predictive maintenance [44].

E. Energy harvesting and storage

With the fast development of energy harvesting technology, micro nano or scale-up energy harvesters have been proposed to allow sensors or internet of things (IoT) applications with self-powered or self-sustained capabilities. Facilitation within smart homes, manipulators in industries and monitoring systems in natural settings are all moving toward intellectually adaptable and energy-saving advances by converting distributed energies across diverse situations. The development of innovative energy harvesting and storage solutions can complement autonomic computing systems in smart buildings, further contributing to energy efficiency, sustainability, and resilience [45].

In conclusion, the future of autonomic computing in smart buildings holds significant promise, with numerous advancements and opportunities on the horizon. However, addressing the associated challenges in part III will be essential to fully harness the potential of autonomic computing in creating intelligent, sustainable, and occupant-friendly urban environments.

VIII. Ethical Considerations

The implementation of autonomic computing in smart buildings offers numerous benefits, including enhanced efficiency, sustainability, and occupant satisfaction. However, it also raises several ethical considerations that need to be addressed to ensure the responsible and equitable use of this technology. This section analyses the potential ethical implications and discusses privacy, security, and other relevant ethical issues [38].

A. Privacy and data ownership

The extensive use of sensors and data collection in autonomic smart buildings raises significant concerns about occupant privacy. The continuous monitoring of occupant behaviour, preferences, and personal information may lead to intrusive surveillance and potential misuse of sensitive data. To address these concerns, it is essential to [30]:

- Implement strict data privacy policies and ensure compliance with relevant regulations (e.g., GDPR) to protect occupants' personal information.
- Employ anonymisation and aggregation techniques to minimise the risk of identifying individuals from the collected data.
- Provide transparent information to building occupants about the type of data collected, its purpose, and the measures taken to protect their privacy.

B. Security

The increased reliance on interconnected systems and data sharing in autonomic smart buildings heightens the risk of cyberattacks and data breaches. Ensuring the security of these systems is a critical ethical responsibility, as a breach could lead to severe consequences, such as unauthorised access to sensitive data, disruption of building operations, or even threats to occupant safety. To address security concerns [30]:

- Design autonomic computing solutions with built-in security measures, such as robust encryption, authentication, and access control mechanisms.
- Regularly update and patch software and hardware components to protect against known vulnerabilities.
- Conduct periodic security audits and risk assessments to identify potential threats and implement necessary countermeasures.

C. Accountability and Responsibility

As autonomic computing systems are capable of making decisions and taking actions with minimal human intervention, it raises questions about accountability and responsibility when things go wrong. Determining who is responsible for the system's actions, whether it is the system developers, building owners, or operators, can be challenging. To address this issue [38]:

- Develop clear guidelines and policies that define the roles and responsibilities of all stakeholders involved in the design, implementation, and management of autonomic computing systems in smart buildings.
- Ensure that autonomic systems are transparent and explainable in their decision-making processes, enabling easier assessment of accountability when issues arise.
- Establish a regulatory framework to govern the development and deployment of autonomic computing systems, ensuring adherence to ethical principles and responsible technology use.

D. Digital Divide and Inclusivity

The implementation of autonomic computing in smart buildings may inadvertently exacerbate the digital divide, as not all communities or individuals have equal access to advanced technologies and their benefits. Ensuring inclusivity and equal opportunity is an important ethical consideration. To promote inclusivity [46]:

- Strive to make autonomic computing solutions accessible and affordable for a diverse range of building types and communities, including low-income and underprivileged areas.
- Develop user interfaces and interaction mechanisms that cater to the needs of all building occupants, including those with disabilities or special requirements.
- Encourage participation and consultation with diverse stakeholders, including local communities, in the design and implementation of autonomic computing solutions to ensure their needs and concerns are addressed.

In conclusion, by considering and addressing privacy, security, accountability, and inclusivity concerns, we can create a more ethical foundation for the future development and deployment of autonomic computing in smart buildings.

IX. Conclusion

This research examined the potential of autonomic computing in smart buildings, focusing on the challenges, opportunities, and ethical aspects of its implementation. The main findings are as follows:

- Autonomic computing offers substantial benefits for smart buildings, such as energy efficiency, enhanced occupant comfort, and reduced operational costs. Its self-configuration, self-optimization, self-healing, and self-protection capabilities allow buildings to adapt to complex environments and occupant needs. - Current limitations and challenges in applying autonomic computing to smart buildings include implementation complexity, interoperability, security and privacy concerns, and high initial investment. Real-world examples demonstrate the impact of these challenges on the adoption and integration of autonomic computing solutions. - The proposed Adaptive Smart Building Management System (ASBMS) serves as a proof of concept for integrating autonomic computing in smart buildings while addressing the identified challenges. Key components of ASBMS include a sensor and actuator network, data management and processing layer, autonomic controller, user interface, and security and privacy module. - Future predictions for autonomic computing in smart buildings emphasize advancements in AI and machine learning, the proliferation of IoT devices and sensors, edge computing and 5G connectivity, digital twin technology, and energy harvesting and storage. However, scalability, standardization, data privacy, and legal and ethical considerations remain challenges to be addressed. - Ethical considerations in implementing autonomic computing in smart buildings encompass privacy, security, accountability and responsibility, and digital divide and inclusivity. Addressing these concerns is essential for ensuring responsible, equitable, and inclusive technology use.

In conclusion, autonomic computing possesses enormous potential for revolutionizing smart buildings, providing significant benefits in efficiency, sustainability, and occupant satisfaction. To unlock the full potential of autonomic computing, and to address the ethical concerns, developments in areas mentioned below are required:

1. Invest in developing and standardizing open-source platforms and communication protocols to enable seamless integration of diverse systems and components in smart buildings.

2. Advance AI and machine learning techniques, as well as edge computing and 5G connectivity, to enhance the performance and responsiveness of autonomic computing solutions.

3. Prioritize security and privacy in the design of autonomic computing systems, incorporating advanced encryption, authentication, and access control mechanisms to protect sensitive data and building systems.

4. Establish clear guidelines, policies, and regulations to address accountability and responsibility concerns and ensure responsible technology use.

5. Encourage accessibility and Being inclusive in developing and deploying autonomic computing solutions, catering to various building types, communities, and occupant needs.

Additionally, we have reviewed the impact of AI in protecting smart building technologies, which led to proposing a framework for smart homes integrating security mechanisms and introducing AI-based algorithms to detect common cyber threats. Although the research is in its early stages, future research will evaluate the efficiency and accuracy of the reviewed AI algorithms to investigate the feasibility of using this information in forensic data, potentially allowing investigators to extract digital evidence without invading personal devices. This approach could support the development of reliable chains of custody while protecting personal data. By addressing these recommendations, we can pave the way for a more intelligent, sustainable, and occupant-friendly future for smart buildings through the responsible integration of autonomic computing.

References

[1] Saad al-sumaiti, A., Ahmed, M.H. and Salama, M.M., 2014. Smart home activities: A literature review. Electric Power Components and Systems, 42(3-4), pp.294-305.

[2] https://en.wikipedia.org/wiki/Autonomic computing

[3] Reisinger, M.R., Prost, S., Schrammel, J. and Fröhlich, P., 2022. User requirements for the design of smart homes: dimensions and goals. Journal of Ambient Intelligence and Humanized Computing, pp.1-20.

[4] Yan, B., Hao, F. Meng, X. When artificial intelligence meets building energy efficiency, a review focusing on zero energy building. Artif Intell Rev 54, 2193–2220 (2021). https://doi.org/10.1007/s10462-020-09902-w

[5] Stakeholder Engagement for Smart Cities and Digital Infrastructure Projects: National Guidance Document Dr Richmond Ehwi Dr Hannah Holmes Dr Sabina Maslova June 2020

[6] Georgievski, I., Shahid, M.Z. and Aiello, M., 2023. AI temporal planning for energy smart buildings. Energy Informatics, 6(Suppl 1), p.18.

[7] Kar, P., Kumar, A., Shareef, A. et al. An intelligent lighting control system for individual visual comfort and energy savings in buildings. J Reliable Intell Environ 9, 385–398 (2023). https://doi.org/10.1007/s40860-022-00189-y

[8] AUTONOMIC COMPUTING: A LONG TERM VISION IN COMPUTING Sandeep Kumar Chauhan* and Dr Arun Sharma Research Scholar Mewar University Chittorgarh, Rajasthan Professor and Head, Dept. of Comp. Sc. and Engg., Krishna Inst. of Engg. and Tech., Ghaziabad
[9] https://www.techopedia.com/2/32077/enterprise/data-centers/the-past-present-and-future-of-autonomic-computing
[10] Review on the Application of Artificial Intelligence in Smart Homes Xiao Guo 1,2 , Zhenjiang Shen 1,2,*, Yajing Zhang 1,2 and Teng Wu 1,2 1 Joint International Laboratory Of Spatial Planning And Sustainable Development (FZUKU-LAB SPSD), Fuzhou 350108, China School of Natural Science and Technology, Environmental Design Division, Kanazawa University, Kanazawa City 920-1192, Japan
[11] Gura, N., Patel, A., Wander, A., Eberle, H. and Shantz, S.C., 2004. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6 (pp. 119-132). Springer Berlin Heidelberg.
[12] Naik, N., 2017, October. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In 2017 IEEE international systems engineering symposium (ISSE) (pp. 1-7). IEEE.
[13] https://forum.ovoenergy.com/smart-meters-136/smart-meters-working-but-not-communicating-with-ovo-why-435/index3.html
[14] Bugeja J, Jacobsson A, Davidsson P (2016). On privacy and security challenges in smart connected homes. In: 2016 European intelligence and security informatics conference (EISIC).IEEE, pp 172–175.
[15] Bafandehkar M, Yasin SM, Mahmod R, Hanapi ZM (2013) Comparison of ECC and RSA algorithm in resource constrained devices. In: 2013 International conference on IT convergence and security (ICITCS). IEEE, pp 1–3.
[16] Greenberg A (2020) Hackers can use lasers to 'speak' to your amazon echo. Wired. https:// www.wired.com/story/lasers-hack-amazonecho-google-home/. 5 Oct 2020.
[17] Karimi K, Krit S (2019) Smart home-smartphone systems: threats, security requirements and open research challenges. In: 2019 International conference of computer science and renewable energies (ICCSRE). IEEE, pp 1–5
[18] Guo X, Shen Z, Zhang Y, Wu T (2019) Review on the application of artificial intelligence in smart homes. Smart Cities 2(3):402–420
[19] Asokan N, Niemi V, Nyberg K (2003) Man-in-the-middle in tunnelled authentication protocols. In: International workshop on security protocols. Springer, Berlin, Heidelberg, pp 28–41
[20] Singh S, Jeong YS, Park JH (2016) A survey on cloud computing security: Issues, threats, and solutions. J Netw Comput Appl 75:200–222
[21] Dougan T, Curran K (2012) Man in the browser attacks. Int J Ambient Comput Intell (IJACI) 4(1):29–39
[22] Jacobsson A, Boldt M, Carlsson B (2016) A risk analysis of a smart home automation system. Futur Gener Comput Syst 56:719–733
[23] Becks, E., Zdankin, P., Matkovic, V. and Weis, T., 2023. Complexity of Smart Home Setups: A Qualitative User Study on Smart Home Assistance and Implications on Technical Requirements. Technologies, 11(1), p.9.
[24] Davies, E.I. and Anireh, V.I.E., 2019. Design and Implementation of Smart home System using Internet of things. Journal of Digital Innovations Contemporary Research In Science., Engineering Technology, 7(1), pp.33-42.
[25] El-Azab, R., 2021. Smart homes: Potentials and challenges. Clean Energy, 5(2), pp.302-315.
[26] Jnr., B.A., Sylva, W., Watat, J.K. et al. A Framework for Standardization of Distributed Ledger Technologies for Interoperable Data Integration and Alignment in Sustainable Smart Cities. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01554-9
[27] Hamid Jahankhani Arshad Jamal Shaun Lawson Editors Cybersecurity, Privacy and Freedom Protection in the Connected World Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021
[28] Smart Building Management System (SBMS) for Commercial Buildings—Key Attributes and Usage Intentions from Building Professionals' Perspective King Hang Lam 1,* , Wai Ming To 2 and Peter K.C. Lee 3
[29] Eini, R., Linkous, L., Zohrabi, N. and Abdelwahed, S., 2021. Smart building management system: Performance specifications and design requirements. Journal of Building Engineering, 39, p.102222.
[30] Internet of Things IoT through a Multi-disciplinary Perspective 5th IFIP International Cross-Domain Conference, IFIPIoT 2022 Amsterdam, The Netherlands, October 27–28, 2022 Proceedings
[31] Ciholas, P., Lennie, A., Sadigova, P. and Such, J.M., 2019. The security of smart buildings: a systematic literature review. arXiv preprint arXiv:1901.05837.
[32] Autonomic Computing, IBM White Paper, June 2005 Third Edition, An architectural blueprint for autonomic computing.
[33] https://new.abb.com/innovation/abb-ability-smart-sensor
[34] https://www.se.com/hk/en/about-us/sustainability/
[35] Guo, X., Shen, Z., Zhang, Y. and Wu, T., 2019. Review on the application of artificial intelligence in smart homes. Smart Cities, 2(3), pp.402-420.
[36] Yu, X., Zhang, Q., Zhang, X. et al. Microbial self-healing of cracks in cement-based materials and its influencing factors. Front. Struct. Civ. Eng. (2023). https://doi.org/10.1007/s11709-023-0986-6
[37] https://drexel.edu/news/archive/2023/June/AI-damage-detection-reinforced-concrete-cracking-patterns
[38] Pirzada, P., Wilde, A., Doherty, G.H. and Harris-Birtill, D., 2022. Ethics and acceptance of smart homes for older adults. Informatics for Health and Social Care, 47(1), pp.10-37.
[39] https://www.delltechnologies.com/asset/en-us/solutions/industry-solutions/customer-stories-case-studies/dell-desigo-siemens-case-study.pdf
[40] https://www.ibm.com/about/innovation-studio/munich
[41] https://edge.tech/developments/the-edge
[42] https://plparchitecture.com/
[43] Matinkhah, S.M. and Shafik, W., 2019, December. Smart grid empowered by 5G technology. In 2019 Smart Grid Conference (SGC) (pp. 1-6). IEEE.
[44] Asvadi, A., Mitriakov, A., Lohr, C. and Papadakis, P., 2022, June. Digital Twin Driven Smart Home: A Feasibility Study. In International Conference on Smart Homes and Health Telematics (pp. 18-29). Cham: Springer International Publishing.
[45] Liu L, Guo X, Liu W, Lee C. Recent Progress in the Energy Harvesting Technology-From Self-Powered Sensors to Self-Sustained IoT, and New Applications. Nanomaterials (Basel). 2021 Nov 5;11(11):2975. doi: 10.3390/nano11112975. PMID: 34835739; PMCID: PMC8620223.
[46] Shams, R.A., Zowghi, D. Bano, M. AI and the quest for diversity and inclusion: a systematic literature review. AI Ethics (2023). https://doi.org/10.1007/s43681-023-00362-w

X. Figures and tables

- Fig 1 is a table that shows a comparison between messaging protocols used in IoT systems
- Fig.2 Secure smart home network architecture
- Fig.3 Smart home network architecture
- Fig.4 Data Flow Diagram of the Proposed System
- Fig.5 Autonomic Computing reference Architecture
- Fig.6 Functional detail of the Autonomic Manager

Protocol	MQTT	CoAP	AMQP	HTTP
Year	1999	2010	2003	1997
Header size	2 Bytes	4 Bytes	8 Bytes	Undefined
Message size	up to 256 MB maximum size	Normally small to fit in a single IP datagram	Negotiable and undefined	Large and undefined (depends on web server or programming technology)
Semantics/Methods	Connect, Disconnect, Publish, Subscribe, Unsubscribe, Close	Get, Post, Put, Delete	Consume, Deliver, Publish, Get, Select, Ack, Delete, Nack, Recover, Reject, Open, Close	Get, Post, Head, Put, Patch, Options, Connect, Delete
Cache/Proxy support	Partial	Yes	Yes	Yes
Quality of Service (QoS) reliability	QoS 0—delive the msg once, with no confirmation QoS 1—deliver the msg at least once, with confirmation required QoS 2—deliver the msg exactly once by using the 4-step handshake	Confirmable Message (similar to QoS 0) or Non-confirmable message (similar to QoS 1)	Settle Format (similar to QoS 0) or Unsettle format (similar to QoS 1)	Limited (via TCP)
Standards	OASIS, Eclipse Foundation	IETF, Eclipse Foundation	OASIS, ISO/IEC	IETF and W3C
Transport Protocol	TCP (MQTT-SN can use UDP)	UDP, SCTP	TCP, SCTP	TCP
Security	TLS/SSL	DTLS, IPSec	TLS/SSL, IPSec, SASL	TLS/SSL
Default port	1883/8883 (TLS, SSL)	5683 – UDP/5684 – DTLS	5671 (TLS/SSL), 5672	80/443 (TLS/SSL)
Encoding format	Binary	Binary	Binary	Text
Licensing model	Open source	Open source	Open source	Free
Organisational support	IBM, Facebook, Cisco, Red Hat, Tibco, ITSO, M2Mi, AWS, Indusoft, Fiorano	Cisco, Contiki, Erika, IoTvity	Microsoft, JP Morgan, Bank of America, Barclays, Goldman Sachs, Credit Suisse	Global Web Protocol Standard

Fig. 1. Messaging protocols used in IoT Systems

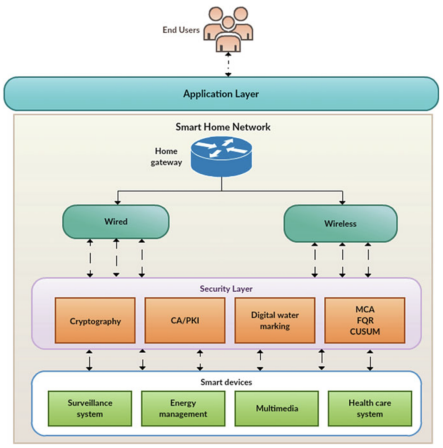

Fig. 2. Secure Smart Home Network Architecture

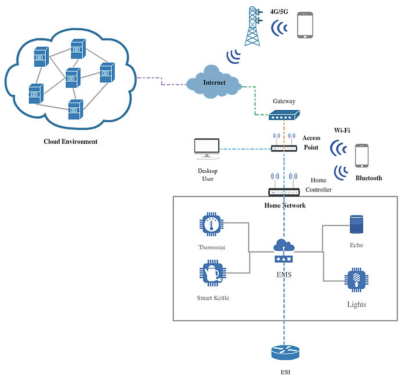

Fig. 3. Smart Home Network Architecture

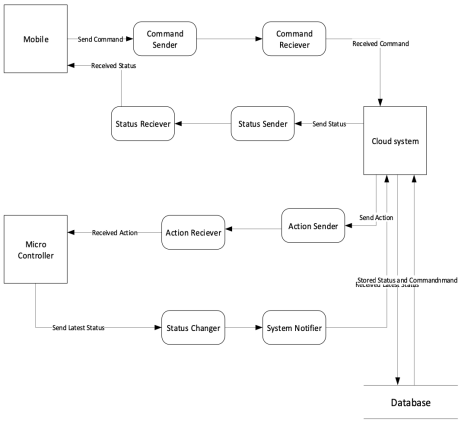

Fig. 4. Data Flow Diagram of the Proposed System

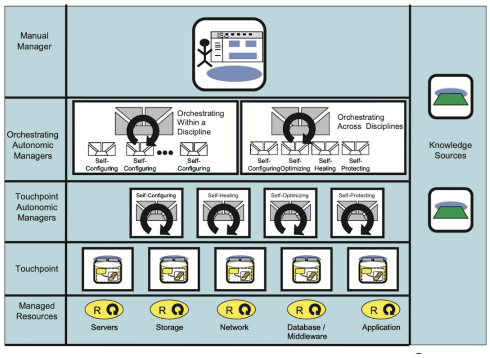

Fig. 5. Autonomic Computing reference Architecture

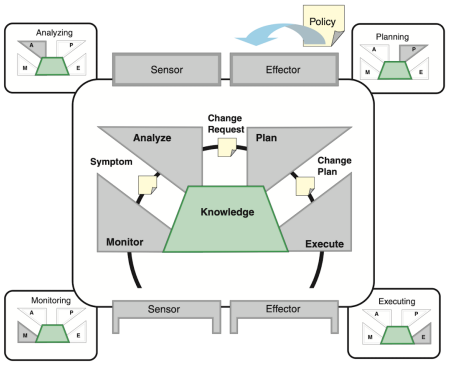

Fig. 6. Functional detail of the Autonomic Manager