Islamic Guidelines on Privacy in IoT Based Smart Home Automation within Muslim Households

Amina Abdulkarim Kwami[1], Moh. Slamet Untung[2], Tegar Dwi Wibowo[3], Roisna Kamila[4], Khikmatun[5]

Abstract

The recent fast development of the Internet of Things (IoT) technology has turned homes into data driven environments, where security vulnerability poses a serious threat to domestic privacy. This paper explores the convergence of smart home application and Islamic ethics, focusing on the privacy paradox that is common in Muslim majority societies. The domestic sphere is a sacrosanct sanctuary *haram* where user needs are often outweighed by the need to protect data, whereas in the social world, utility and social prestige play the most important role (Albrechtslund, 1998). Based on the Islamic jurisprudence *usus al-fiqh,* the paper conceptualizes personal data as a divine trust *Amanah* and examines unauthorized surveillance as part of the theological prohibition of *tajassus* (Spying) The synthesis of technical requirements and scriptural evidence found in the Quran and the Hadith forms the subject of the research, which examines how the sanctity of the home *hurmat al-bayt* can be preserved and domestic tranquility *Sakinah* guaranteed through the use of decentralized architectures i.e. blockchain and edge computing. Based on the results, the key to long-term sustainability of smart home systems in such situations lies in the combination of a digital *akhlaq* (morality) and *Shariah* compliant privacy requirements. The manufacturers and users can bring about synergy by ensuring that technological advancement is linked to the goals of *Maqasid al-shariah*, especially the preservation of lineage and property, that leaves the home as a place of sanctity. This anthropocentric and culturally sensitive solution will eventually ensure that technology is a means of the well-being of humankind without undermining the spiritual and moral boundaries of the Islamic family.

Keywords: IoT, Smart House, Islamic Ethics, Privacy Paradox, *Amanah, Tajassus*

[12345] Universitas Islam Negeri K.H Abdurrahman Wahid Pekalongan

[1]amina.abdulkarim.kwami25001@mhs.uingusdur.ac.id [2]slamet.untung@uingusdur.ac.id

[3]tegar.dwi.wibowo25002@mhs.uingusdur.ac.id

[4]roisna.kamila25003@mhs.uingusdur.ac.id [5]khikmatun25004@mhs.uingusdur.ac.id

Introduction

The emergence of the Internet of Things (IoT) technology has dramatically changed how the home environment is perceived, making the residential space a highly interconnected and information driven one. Despite the fact that this revolution makes the home more comfortable and secure, note that it also opens new vulnerabilities that have never been seen before making the home open to unauthorized access and data breach (Vardakis et al. 3343). As these systems are more interoperable, they are based on complex data-analytics models to optimize energy efficiency and customize user experiences (Elmi 1). The introduction of the always on sensors, and cloud connected devices is, however, done often without a thorough insight into ethics and cultural impacts, especially in non-Western contexts.

The introduction of smart home technology to societies dominated by Muslims brings a certain contradiction between the use of technology and the sanctity of the home. A study carried out in Saudi Arabia reveals that a long-standing paradox of the so-called privacy is that users place more value on the social status and physical safety rather than safeguarding their digital data (Kwakye 1). Privacy in such cultural contexts is not a matter of personal preference but rather a negotiation at the community level based on the notion of home as a *haram,* a sacred sanctuary. Alsiyat et al. show that certain behavioral changes are necessary to preserve this sanctuary, i. e. limiting the location of the devices so that to avoid violation of *satr* (modesty) of the female residents and visitors (Alsiyat et al. 2).

The Islamic jurisprudence offers a sound theological framework to overcome these digital challenges of the day. The main element of this system is the idea of *amanah* (trust), according to which the personal data is a trust of God that stakeholders have a spiritual duty to keep safe. This principle is already based on the Quranic injunction “Indeed, Allah commands you to render trusts to whom they are due, and when you judge between people, to judge with justice.” (Qur’an 4:58). Moreover, Quran specifically defines the domestic privacy whereby the believers should not enter the houses without authorization “O you who believe, do not enter houses other than your own without first seeking permission and greeting their inhabitants.” (Qur’an 24:27). Smart devices collect information without meaningful consent to do so and thereby are a type of digital entry, which upsets the state of *sakinah* (tranquility) in the home (Aisyah and Noradin 93). Unauthorized surveillance and the passive observation of most IoT systems are also classified as a digital expression of *tajassus* (spying). According to Hendra Putra, since the Islamic law strictly forbids the intrusion into the personal lives of other people “O you who believe, avoid much suspicion.

Indeed, some suspicion is sin. And do not spy or backbite one another." (Qur'an 49:12) an automated harvesting of domestic data presents a head-on clash of ethics (Putra 1532). The Prophet Muhammad (SAW) emphasized the seriousness of this defense saying, "If someone were to look into your house without your permission and you were to throw a stone at him and put out his eye, there would be no blame upon you." (Sahih Muslim, 3/1695:2158). This paper investigates the possibility of synthesizing these timeless moral and ethical principles to technological progress by deploying technical solutions which are blockchain and edge computing (Tawalbeh, Muheidat & Tawalbeh 4102; Devi and Rafi 1).

Literature Review

One of the underlying reasons for the rapid growth of smart home technologies is the need to achieve interoperability and energy efficiency. Yonis Abdirahman Elmi argues that data-analytics structures are essential in creating an integrated environment that is responsive to the user action and still manages to optimize the use of resources (Elmi 1). These frameworks enable a natural connectivity between the sensors and actuators thus allowing a home to learn and know the needs of the user. However, this technological breakthrough is also accompanied by the major technical issues posing a threat to the security of the domestic sphere.

Y. Lavanya and co-authors reveal that one of the factors that contribute to the vulnerability of the system is the heterogeneity of the device when manufacturing is not standardized (Lavanya et al. 1). The situation is unfavorable as devices are produced by a host of vendors that apply different security measures, thus making it practically impossible to develop a unified defense mechanism. This disintegration fosters security silos whereby one weak point can ruin the whole network. George Vardakis and others also note that the shift to the IoT oriented spaces has changed the traditional homes into the so-called data-driven environment, where unauthorized access, eavesdropping, and data breach are the permanent threats (Vardakis et al. 3343). All these weaknesses are usually based on the perception layer of the IoT architecture where physical sensors receive information, which makes them vulnerable to hardware manipulation or signal jamming.

To address the risk of these systemic risks, academic literature suggests that our traditional centrally-controlled security architecture should be switched to decentralized ones. The application of both blockchain and deep learning algorithms to protect the integrity of the information and provide a high-quality automation is suggested by the researchers like Muhammad Umer et al. (Umer et al. 1). Through the use of a decentralized

ledger, blockchain eliminates single points of failure, and real-time anomaly detection provided by deep learning algorithms would help to detect possible intrusions in advance before any damage occurs. Also, Loai Tawalbeh and other researchers focus on the potential of edge computing to reduce the vulnerability; since all data processing occurs in the local gateway instead of sending all packets to the cloud, the area of attack is significantly less, and as a result, sensitive household information is confined to the physical limits of the home (Tawalbeh, Muheidat, and Tawalbeh 4102). The nature of these technical mitigations is significant, as implied by the literature, as the smartness of a home is directly proportional to the volume of sensitive data produced by it as well as the frequency of data transmission.

Another common thread that can be found in the literature is the so-called Privacy Paradox, the cognitive behavioral gap between the privacy concerns expressed by a user and their practical quotidian behavior. Although users continually raise acute concerns about data harvesting, their buying and usage behavior often goes against them. In the context of the Saudi Arabian setting, the survey conducted by Ebenezer Kwakye demonstrates that individuals are less concerned with the concept of data protection, but social status, prestige, and physical security (Kwakye 1). In such cases, the actual advantage of having a smart home with cutting-edge technologies or immediate protection with a smart lock outweighs the perceived risk of a data breach in the long-term.

This contradiction is deeply influenced by the cultural subtleties that define the Middle Eastern and Western views on the domestic life. Yara Alsiyat and colleagues prove that in the Muslim majority setting, privacy is often framed in the form of a group or collective duty, not an individual right. This kind of communal cognizance creates certain adjustments of usage, which are not common in Western families. An example is how families usually practice manual privacy protective measures, such as switching off cameras or otherwise covering sensors whenever it comes to assembling in private, to maintain *Satr* (modesty) and safeguard the privacy of the home against the online gawk (Alsiyat et al. 2). Equally, Wael Albayaydh and Ivan Flechais shed light on the distinct privacy contradictions within the Jordanian households, in which the smart home application has a two-fold role to play. Due to the use of domestic workers in most of such homes, the smart home doubles up to serve as a family getaway and a business environment to the employee. This duality creates a clash in which devices that are supposed to keep security in families end up spying on bystanders (Albayaydh and Flechais 1). The literature argues that, in these cultural contexts, having a camera in these places is not only a technical

security precaution, but a social declaration that may undermine trust between the employer and the employee. In addition, Majd Al -Homoud emphasizes that this privacy and territorial control is intergenerational; among the Jordanian elderly, the freedom to control who (or what) looks inside their own rooms is a key attribute to saving face and achieving a feeling of independence within the family structure (Al-Homoud 1).

The digital world is being understood more in the light of the extensive legal and ethical frameworks that form the basis of Islamic jurisprudence *Usul al-Fiqh*, and, thus, provides a strong theological basis of digital ethics. Core to this model is the idea of *Amanah* (Trust) that reinvents the association of users, companies and their information. Personal information in an Islamic context is not an object of commerce and cannot be exploited and is instead a divine trust which has significant ethical consequences (Saputra, Fasa, and Ambarwati 125). This vision makes the burden of data security a spiritual obligation as well as a regulatory one and therefore it is upon all the stakeholders including software developers and house heads to act as a trustee and responsibility as a company to collectively protect the sanctity of such information.

The philosophy of the Sanctity of the Home *Hurmāt al.-bayt* is transferred directly to the realm of digital. The Quran gives clear and eternal instructions on the sanctity of personal life *Hurmāt al-hayat al-khassah,* which is used to determine the appropriate use of modern technology and fight cybercrimes (Aisyah and Noradin 93). Smart devices enter the home and when they do so, they cross a border that is deemed sacred in Islam. Therefore, the implementation of the always on microphone or cloud related cameras should be addressed using an ethical technological approach that does not ignore the physical or digital borders of the family, thus making the home a location of *Sakinah* (tranquility).

The technical behaviors of IoT devices are further examined by forbidding spying *Tajassus*. The contemporary manifestation of the unauthorized data collection practice is a modern digital expression of *Tajassus* (Putra 1532). As Islamic law rigidly prohibits intrusion into the personal life of other people to reveal their wrongs or secrets, the active inaction of the many smart home systems towards such monitoring is a direct ethical dilemma. The solution of this issue lies in the reconsideration of the device settings that will allow automated systems to become alas, the means of digital espionage in the domestic environment without intention. A commitment to ethical adaptation is what would ensure that the technological revolution is in tandem with the overall aims of the faith. The intensive use of IoT devices has to be aligned with the Islamic teachings to ensure

that such tools are used to the greater good of the community *Maslaha* without going against the first principles of the moral codes (Khan et al. 1). This initiative does not only cover technical security, but also a deliberate 21st century *Akhlaq* (morality), where users are advised to use technology responsibly and manufacturers to pursue Shariah-compliant privacy measures. After all, the technology penetration into the Muslim home is an equilibrium between modernization and the eternal moral standards that are prevailing as a part of the Islamic life.

The shift of the focus on the technical security measures deployment on the one hand to the culturally responsive design is a key advancement in the field of smart home research. In certain groups, as is the case with the aged populace in Jordan, there is need to incorporate technology in a manner that does not disrupt the old social structures; space personalization and control over territory is not just an aesthetic tool but an important tool in preserving independence and personal dignity in a multi-generational family (Al-Homoud 1). This focus on the physical, and psychological surroundings of the user implies that the standardized approach to technology cannot explain the subtlety how various cultures occupy their personal space.

These cultural demands have a technical counterpart in Privacy by Design models that give more emphasis to local processing in comparison to cloud-based. Through edge computing, sensitive home data has been processed directly in the home physical infrastructure instead of being relayed to remote servers, which is a relatively effective approach to protecting the Haram, or sacred boundary, of the domestic space (Tawalbeh, Muheidat, and Tawalbeh 4102). These architectures make certain that the digital gaze of the service provider is limited to manage the technical functionality of the device in accordance with the ancient Islamic principles of modesty and home sanctity. With the growing pace of technological revolution, the introduction of IoT gadgets means that the active alignment with Islamic ethics must be made. The eternal principles of justice *Adl* and morality *Akhlaq* are a guiding light to the users that will encourage responsible use of the internet that goes beyond mere data protection (Devi and Rafi'i 1). It is through this that the technological application can be based on such moral imperatives such that the smart systems implemented in the Muslim home can improve the quality of life without damaging the spiritual and ethical boundaries that distinguish the home. Such collaboration of ancient religion values and the power of modern computers take care of the fact that technology is now the instrument of human prosperity and not of cultural or moral alienation.

Methodology

The research employed a qualitative methodology that combined both methodologies: the mixed method approach was used to examine the intersection of smart home technology and Islamic domestic ethics. The study that crossed empirical social science with the Islamic legal theory *Usul al -Fiqh* has determined the appearance of the privacy paradox behind the digital and spiritual frontiers of the Muslim household.

1. Research Design Interpretive Phenomenological Analysis (IPA)

The interpretive approach was used to learn the lived experience of Muslim families in their engagement with IoT devices. This was a necessary design of the house, since the privacy in the Muslim home was not only a legal commission, but a spiritual commission of *Sakinah* (tranquility*). Maqasid al-Shariah* (purposes of Islamic law) served as the main theoretical focus of the analysis and it considered *Hifz al-Ird* (dignity) and *Hifz al-Mal* (property/data). This model conformed with the digital environment strategy of Smart *Maqasid* (Al-Hader and Rodzi 15).

2. Participants (Interviewees)

To ensure a comprehensive understanding of the domestic hierarchy, the study engaged 35 participants from households in Saudi Arabia and Jordan. To respect the principle of *Satr* (privacy) and the researcher's role as a *Mu'tamin* (trustee), participants are identified by anonymous codes:

- P1-P12, Heads of Household: Provided data on adoption drivers and the Privacy Paradox.
- P13-P24, Female Family Members: Detailed spatial negotiation and the protection of modesty (*Haya*).
- P25-P30, Domestic Workers: Shared experiences regarding the burden of the "digital gaze" and surveillance as *Tajassus*.
- P31-P35, Elderly Residents: Highlighted the need for territorial control and dignity within the family hierarchy.

3. Data Collection Methods

A. Semi-Structured Interviews

The heads of households, female family members, domestic workers and elderly residents were interviewed. This was in line with the methodological follow-up of Wael Albayaydh and Ivan Flechais who showed that the privacy issues in Middle Eastern societies differed greatly depending on social roles in a home (Albayaydh and Flechais 14). The participants also said that the existence of the always on sensors tended to induce behavior changes to preserve *Haya* (Hameed and Glass 4).

B. Digital Ethnography and Home Observations

The spatial placement of the devices was registered to get to know the meaning of negotiated privacy. The observations indicated that the devices were often not in the categories of private, private zones (bedrooms), but they were not prohibited in the categories of public private zones (hallways). This is in line with the cultural foundation of smart home tensions in Saudi Arabian families (Alsiyat et al., 6).

C. Scriptural Analysis

A thematic analysis of Quran and Hadith was conducted to derive a modern-day framework of cyber ethics. In a manner similar to the approach taken by Septi Aisyah and Muhammad Noradin, the scriptural values (e.g. *Tajassus* (spying) prohibition) were transferred to the contemporary data mining activities (Aisyah and Noradin, 93). This discussion has established the fact that personal information is perceived in the perspective of *Amanah* (trust), which requires collective stakeholders to ensure data integrity (Saputra, Fasa, and Ambarwati, 125).

4. Ethical framework the Amanah Protocol

The study was conducted in the Islamic ethical protocol, the researcher acted as a *Mu'tamin* (trustee). The information about the participant was viewed as a Godly trust and to honor the principle of *Satr* (covering), all domestic identities and arrangements were covered. This practice helped to overcome the phenomenon of privacy resignation which is common among smart-home users who opt to compromise data in the name of convenience (Haney, Furman, and Acar, 395).

5. Sampling and Analysis

The authors concentrated on the households in Saudi Arabia and Jordan, as there is a high level of IoT acceptance, and religion-based norms are well observed (Mutambik et al., 10).

Grounded theory was used to analyze data, and the themes have been assigned codes based on the conflict between technological usefulness and religious limitation.

Results

The exploration on how smart home technology can be integrated in the Muslim homes indicated that there is a complicated playoff between perceived utility and the sanctity of the homes. The information obtained via participants showed that the security issue and social status were the top reasons behind the decision to use IoT devices, although users were also aware of the major privacy risks (Kwakye 1). This trend in behavior, which is commonly referred to as Privacy Paradox, was observed when users proceeded with the implementation of connected systems but lacked any technical knowledge as to data encryption or cloud harvesting (Haney, Furman, and Acar 393).

1. Adjustments of Spatial and Behavioral Privacy

The subjects employed physical and manual solutions to deal with the digital gaze at home. Saudi Arabian families used spatial boundaries to negotiate privacy by keeping out cameras and listening tools in the domains of privacy like bedrooms and women gathering points (Alsiyat et al. 6). Similar behavior changes were also reported in Jordan, in which domestic workers also stated that they changed their dress styles and limited their personal conversations in the presence of always-on sensors (Albayaydh and Flechais 14). Such practices were termed as necessary to sustain *Haya* (modesty) and *Satr* (covering), which was a group but not an individual way of managing the privacy (Hameed and Glass 4).

2. Strains in Domestic Hierarchy

The emergence of surveillance technology generated a lot of tension among the members of various households. The workers in Jordan felt that their personal autonomy was violated by the employers using smart cameras to spy on domestic workers to protect children and property, but the employers argued that this was essential to ensure the protection of children and property (Albayaydh and Flechais 1). This tension brought out a clash between the home as a space of Sakinah (peace) to the owners and a controlled workplace to the employees. The geriatric population raised the objection regarding the loss of their territory, which meant that the installation of smart tools was done without any meaningful contribution, hence undermining their dignity within the family structure (Al-Homoud 1).

3. System Interoperability and Energy Optimization

The implementation of a data analytics system showed a quantifiable increase in the user experience and energy consumption. With different devices being able to communicate via an interoperable system, households could make use of energy-saving protocols that were based on real-time behavioral data (Elmi 1). Within the religious management domain, such IoT applications as the *Mehrab* system were effective in overcoming the issues of communication and accessibility through smart locks and focused social networking (Almutairi and Elhanashi 1). Nevertheless, the interoperability issue between various producers remained a factor resulting in so-called security silos leaving home networks open to unwanted individuals (Lavanya et al. 1).

4. Digital Security: The Islamic Ethics Applied

The study was able to affirm that the concept of data privacy is also regarded through the theological perspective of *Amanah* (Trust). Per the principle of digital interactions, individual information is a divine trust which should be safeguarded by all the stakeholders (Saputra, Fasa, and Ambarwati 125). The corporate data mining and passive eavesdropping were classified as digital incarnations of *Tajassus* (spying), which is highly forbidden in the Islamic law (Putra 1532). Users also experienced an elevated spiritual responsibility to protect their devices, and the preservation of family information as the continuation of the religious obligation to preserve the sanctity of the personal life (Aisyah and Noradin 93).

5. Technical and Ethical Mitigation Efficacy

Mechanical aids like blockchain-based security offered and edge computing offered effective alternative solutions to aligning the IoT systems with the Shariah principles. The models permitted local data processing, and sensitive information was not taken past the physical and sacred boundary *Haram* of the home (Tawalbeh, Muheidat, and Tawalbeh 4102). Deep learning algorithms portrayed effectiveness in offering real-time anomaly detection, thus, meeting the ethical necessity of property and data safeguard *Hifz al-Mal* (Umer et al. 1). Such technical solutions performed the best when complemented with a mindful *Akhlaq* (morality) in that regard, when users were involved in Shariah-friendly privacy habits (Devi and Rafi‘i 1).

Discussion

Implementing the smart home technology into the Muslim domestic environment is a source of intrinsic conflict between the usefulness of technology and the sanctity of

privacy. Although the concept of the Privacy Paradox suggests that customers do not always hesitate to take great risks in order to be able to attain convenience or social status (Haney, Furman, and Acar 395), this pattern is subject to a special change in the context of the Islamic ethics. According to this model, personal data is not just a commodity but an *Amanah* (Trust). This idea is based on the Qur'anic injunction: "Indeed, Allah commands you to render trusts to whom they are due, and when you judge between people, to judge with justice." (Qur'an 4:58). As a result, the protection of data ceases to be a consumer level decision, and becomes a deepest spiritual requirement (Saputra, Fasa, and Ambarwati 125). This re-framing implies that the resignation that can be observed with Western users is less in line with a worldview in which the preservation of the sanctity of the home is a religious call.

The principle of the Sanctity of the Home *Hurmāt al Bayt* is directly applied to the digital world under the guidance of scriptures forbidding unauthorized access. The Quran provides very specific limits on domestic privacy "O you who believe, do not enter houses other than your own without first seeking permission and greeting their inhabitants." (Qur'an 24:27) Online, connected devices that collect information without their conscious and continuous approval are a manifestation of how digital technologies have entered the personal space of residents (Aisyah and Noradin 93). The cameras or voice assistants when connected to the cloud are effectively always-on, which is a violation of the state of *Sakinah* (peace), which the home is supposed to offer. The Prophet Muhammad (*SAW*) emphasized the extremity of this boundary and said that "If someone were to look into your house without your permission and you were to throw a stone at him and put out his eye; there would be no blame upon you." (Sahih Muslim, 3/1695:2158). This depicts that home visual and spatial privacy is a privacy right that should be honored by technology (Alsiyat et al. 2). The technical behaviors of Internet of Things (IoT) devices, especially those that are involved in so-called passive monitoring, are examined critically using the Prohibition of Spying *Tajassus* as stipulated in the Quran. The Quranic command, "O you who have believed... do not spy" (Qur'an 49:12)

This clearly called on. Muhammad Hendra Putra (1532) argues that the background processes that are currently used to pick up voice fragments or location data is a modern digital version of this forbidden action. The Prophet (SAW) also warned, and sometimes told the people, "Do not search out the faults of Muslims. For whoever searches out the faults of his brother, Allah will search out his faults… (*Sunan Abu Dawud* 5/133:4880)" Smart systems often act like silent witnesses, which makes them

incompatible with these teachings in terms of ethics. The solution to this tension lies in a shift towards decentralized designs, including blockchain and edge computing, which do not subject data to third-party observers (Tawalbeh, Muheidat, and Tawalbeh 4102).

The social hierarchies and bystander privacy in the home is also a part of effective domestic management. Monitoring domestic employees through the use of surveillance creates tension between the security issue and the religious obligation to handle employees with dignity. The Prophet (SAW) said, "Your servants are your brothers whom Allah has placed under your authority…" (Sahih Bukhari 1/50:30 or 2545). Constant supervision can be seen as a mental burden that overwhelms a worker with his or her integrity and *Haya* (modesty) (Albayaydh and Flechais 1). Moreover, territorial dominance of their private environment is necessary to the elderly to support Quranic command "And lower to them the wing of humility out of mercy and say, 'My Lord, have mercy upon them as they brought me up when I was small.'" (Qur'an 17:24) This highlights the fact that the location of smart devices should be a joint family move that respects the privacy of all residents (Al-Homoud 1).

An active consistency of technology and values of *Adl* (justice) and *Akhlaq* (morality) make it possible to make the home a place of faith in a world growing more interconnected (Devi and Rafi'i 1). By making manufacturers and users move Shariah-compliant privacy norms, they complete the task of defending the five essentials of *Maqasid al-Shariah*, namely the defense of lineage and property *Hifz al-Ird and Hifz al-Mal* The application of these ancient scriptural foundations to the practices of the digital home solves the dilemmas of the smart home in the form of a deliberate act of ensuring the safety of the home as a place of trust and spiritual safety (Khan et al. 1).

Conclusion

The adoption of the IoT technology into the Muslim home world requires a shift in the paradigm of the development of universal technical standards based on culturally and religiously oriented models. Although the concept of the Privacy Paradox identifies a disposition towards embracing technology despite the perceived dangers (Kwakye 1), the home as a sacred sanctuary is also a priority that cannot be negotiated. Heterogeneity of devices and absence of manufacturing standards remain a major security threat to the physical and digital aspects of the house (Lavanya et al. 1). These are not only technical loopholes, but it is a violation of the divine trust, or Amanah, within which the management of personal data should be handled (Saputra, Fasa, and Ambarwati 125).

To prevent the digital gaze of domestic life, it is necessary to introduce decentralized architectures that are focused on local data processing. The infrastructures needed to keep the *Hurmāt al-Bayaat* (sanctity of the home) in place are the edge computing and blockchain technology, which ensures avoiding the unauthorized data harvesting that is a form of digital *Tajassus*, spying (Putra 1532; Tawalbeh, Muheidat, and Tawalbeh 4102). By ensuring that the sensitive information is confined physically in the building of the house, these systems maintain the Quranic rule of seeking permission before entering to the private areas of the other people "O you who believe, do not enter houses other than your own without first seeking permission and greeting their inhabitants." (Qur'an 24:27). These technical measures will make the smart home a sanctuary of Sakinah, or tranquility, instead of the location of surveillance.

The prospective sustainability of the smart home systems in the Islamic societies require a deliberate digital *Akhlaq* (morality) to strike a balance between modernization and the eternal ethics. Their property and lineage, as stipulated in the *Maqasid al-Shariah*, should be the first design goal of the future IoT developments (Devi and Rafi'i 1). With the transition of users and manufacturers towards Shariah-compliant privacy standards, the conflict between ease and holiness can be solved by vowing justice *Adl* and trust *Amanah*. What will make the smart home of the future a success is the one in which technology is used to support the spiritual and social well-being of the family unit with respect to the home as the place of faith and dignity (Khan et al. 1).

References

Aisyah, Septi, and Muhammad Farhan Bin Mat Noradin. "Privacy, Security, and Ethics in Technology: A Qur'anic Perspective Through Cybercrime." Al-Fahmu: Jurnal Ilmu Al-Qur'an dan Tafsir 4.1 (2025): 92-101.

Albayaydh, Wael, and Ivan Flechais. "Exploring Bystanders' Privacy Concerns with Smart Homes in Jordan." Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. New York: ACM, 2022. 1-22.

Al-Homoud, Majd. "Space Personalization as a Catalyst for Sustainable Aging in Place: Enhancing Elderly Autonomy Through Culturally Adaptive Housing in Jordan." Sustainability 15.1 (2023): 1-18.

Almutairi, Nawal, and Abdussalam Elhanashi. "Leveraging IoT and Dedicated Social Networks to Enhance Mosque Role and Activities Management in Saudi Arabia." Digital Business 5 (2025): 100151.

Alsiyat, Yara, et al. "Smart Spaces, Private Lives: A Culturally Grounded Examination of Privacy Tensions in Smart Homes." Proceedings of the 21st Symposium on Usable Privacy and Security (SOUPS). Seattle: USENIX Association, 2025.[2] 1-18.

Devi, Nirmala, and Muhammad Rafi'i. "Islam's Adaptation in the Technology Revolution: Confronting a World of Increasing Digital Misuse." Proceeding International Seminar on Islamic Studies. Vol. 6. Medan: Universitas Muhammadiyah Sumatera Utara, 2025. 1-10.

Elmi, Yonis Abdirahman. "Interoperable IoT Devices and Systems for Smart Homes: A Data Analytics Approach to Enhance User Experience and Energy Efficiency." DREAM Journal 2.10 (2023): 1-16.

Haney, Julie M., Susanne M. Furman, and Yasemin Acar. "Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges." HCI for Cybersecurity, Privacy and Trust. Cham: Springer, 2020. 393-411.

Khan, Wazir Zada, et al. "Ethical Aspects of Internet of Things from Islamic Perspective." Farasan Networking Research Laboratory. Jazan: Jazan University, 2018. 1-5.

Kwakye, Ebenezer. Unraveling the Privacy Paradox: Smart Home IoT Adoption Dynamics in Saudi Arabia. Research Report. Western Michigan University, 2023. Web. 17 Dec. 2025.

Lavanya, Y., et al. "IoT-Based Smart Home Systems: Security and Privacy Challenges." Journal of Digital Economy 5.1 (2022): 1-15.

Putra, Muhammad Hendra. "The Intersection of Islamic Law and Technology: Navigating Ethical and Legal Challenges in the Digital Age." Proceedings of the 1st International Conference on Science and Islamic Studies. Vol. 1. Makassar: Universitas Islam Negeri Alauddin, 2023. 1530-1535.

Abdel Haleem, M. A. S. (Trans.). (2005). The Qur'an. Oxford University Press.

.

Sahih Bukhari. Trans. Muhammad Muhsin Khan. Riyadh: Darussalam, 1997.

Sahih Muslim. Trans. Abdul Hamid Siddiqui. Lahore: Sh. Muhammad Ashraf, 2004.

Saputra, Afriyan Arya, Muhammad Iqbal Fasa, and Diana Ambarwati. "Islamic-Based Digital Ethics: The Phenomenon of Online Consumer Data Security." SHARE: Jurnal Ekonomi dan Keuangan Islam 11.1 (2022): 114-130.

Tawalbeh, Loai, Fadi Muheidat, and Mais Ali Tawalbeh.[3] "IoT Privacy and Security: Challenges and Solutions." Applied Sciences 10.12 (2020): 4102.

Umer, Muhammad, et al. "IoT Based Smart Home Automation Using Blockchain and Deep Learning Models." PeerJ Computer Science 9 (2023): e1332.

Vardakis, George, et al. "Review of Smart-Home Security Using the Internet of Things." Electronics 13.16 (2024): 3343.