Protecting Smart Home from Cybersecurity Threats Strategies for Homeowners

Miguel Botto-Tobar[*1, 2], Sumaiya Rehan[3], Ravi Prakash Verma[4]

[1]Department of Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, 5600 MB, The Netherlands
[2] Research Group in Artificial Intelligence and Information Technology, Department of Mathematics and Physical Sciences, University of Guayaquil, Guayaquil, 090514, Ecuador
[3,4]Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow, India

Emails: m.a.botto.tobar@tue.nl; sumaiyarehan@bbdu.ac.in, raviprakashverma@bbdu.ac.in

Abstract

Cyberthreat proliferation parallels the rapid surge in smart home usage. While having everything in one place is convenient, it also increases your home's vulnerability to cyber threats. Such an attack could result in bodily harm, the theft of sensitive information, or both. To mitigate the effects of these threats, owners of smart homes can make efforts to prevent cybercriminals from breaking into their premises starting by updating their firmware to the most recent version, creating secure passwords, and enabling two-factor authentication. Second, people should safeguard their gadgets by creating unique user IDs, disabling unneeded functions, and always keeping a tight eye on them. Finally, they must safeguard the facility where they conduct business by installing surveillance equipment, employing electronic locks, and restricting network access. Individuals must take these safeguards, but they must also stay informed about the most recent threats to home cybersecurity and the best strategies to combat them. Smart home device owners should become acquainted with the risks to which their devices are prone and ensure that their devices are updated to the most recent versions of all available software and security upgrades. Collaboration between homeowners, connected device manufacturers, and internet service providers is required to ensure the security of a smart home. Homeowners should research the security features available in smart home devices and only buy from reputable businesses that value consumer privacy and security. As the Internet of Things (IoT) expands and develops, a data privacy standard that meets the criteria of Data protection is in great demand. Safeguarding smart family apps necessitates a community agreement and specific permission from users to store their personal information in the product's database.

Keywords: Attribute-Based Access Control; Cyber Security; Data Protection; Internet of Things; Role-Based Access Control; Smart Home.

1. Introduction

The IoT revolution that is currently shaping modern infrastructure is predicted to have global ramifications by 2025. The anticipated worth of the IoT market ranges from $4 trillion below average to $11 trillion above average, making the sector priceless. Aside from an increase in the usage of radio frequency identification (RFID) and sensors in factories, the arrival of industrial "4.0" has resulted in the widespread adoption of the IoT in both urban and commercial contexts. Real-time data gathered by sensors implanted in equipment and broadcast across a larger network may boost worker efficiency and inventiveness. Because of the enormous volume of data generated and the number of linked devices in the IoT data privacy is a concern [1-2]. Although IoT devices collect potentially helpful data, they may also jeopardize their users' privacy. With the introduction of cutting-edge smart home technologies, new opportunities and difficulties for customer satisfaction emerge.

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

While smart home technologies can help with specific chores, they should be utilized with prudence and in compliance with the terms of service of the app. Information that can be used to identify a person should never be released without the user's permission [3]. Knowing one's rights to object under the EU's general data protection rules can assist users in avoiding situations like this. One such provision, known as the "right to be forgotten," provides that an individual's digital imprint can be wiped under certain circumstances. Cyberattacks are increasingly threatening Internet users' physical safety, financial security, and personal information. Because of the expansion of internet-enabled devices, particularly in "smart homes," the overall number of online gadgets has increased. Smart homeowners should take security precautions to avoid unauthorised entry [4-5]. They are taking precautions by increasing security at their physical location as well as throughout their infrastructure, which includes their network and other technology tools. They must also collaborate with smart home device manufacturers and service providers to improve smart home security and monitor emerging cyber hazards. The necessity for a data protection standard such as the Data protection will increase as the IoT sector grows. A community agreement is essential for smart family apps to be secure, and users' private information should never be stored in the product's database without their explicit permission [6-7]. More individuals should start using smart gadgets that comply with the Data protection, since they protect users' privacy by limiting sensitive data flow between linked devices. The goal of this law is to better protect the personal information of EU residents. The Data protection is one of the regulations and standards that govern the distribution and use of IoT devices. There are also other rules and regulations in place. Organizations such as the National Institute of Standards and Technology (NIST) have developed guidelines to safeguard the safety of our nation's critical infrastructure. A significant component of this system is the protection of internet-connected devices [8]. The template can be downloaded at the following link: The International Organisation for Standardisation (ISO) has also published security rules for IoT devices. There has been some progress in guaranteeing the safety of IoT devices, but there is still a long way to go. The vast number of electronic devices and the sophisticated network of connections between them pose a significant challenge. It may be tough for you to keep track of all your electronic devices and take the necessary security steps, whether at home or at work [9-10]. Emerging technologies tend to advance quickly, which might present several challenges. Because new technology, tools, and procedures are constantly being developed, it can be difficult for regulatory authorities and groups that define industry standards to keep up. Organizations in the corporate, public, and academic sectors will need to collaborate and coordinate their efforts if they are to be effective in addressing these issues. Sharing knowledge about how to protect IoT devices from emerging threats is critical to the plan's success. As part of this endeavor, new technologies and standards are being developed with the goal of making the Internet of Things a more accessible and safer platform [11-12].

The IoT has the potential to have a profound impact on our daily lives and professional activities. We can improve our everyday routines, create more jobs, and live fuller lives if we enable common household items to connect to the internet. However, the exponential growth of IoT devices is seriously jeopardizing internet security. You can protect your house or business from these types of attacks by increasing the security of your Internet of Things devices [13]. To preserve your privacy and security, use complex passwords, enable two-factor authentication, and execute routine firmware updates. You'll also need to be up to date on the latest cybersecurity threats and the best strategies to defend against them. These processes are critical, but we also require legislation and guidelines to govern the use of IoT devices. Compliance with the Data Protection and related standards is critical for IoT device security. To ensure the safety of all devices connected to the Internet of Things, enterprises, governments, and educational institutions must work together. If we follow these recommendations, we may get the benefits of the Internet of Things without jeopardizing our security or privacy.

The expansion of smart homes has led to an increase in cybersecurity vulnerabilities, and it is the responsibility of each individual homeowner to mitigate these risks. As more gadgets connect to the internet, it becomes more difficult to prevent malicious software from accessing networks. Furthermore, there is currently no agreement on the types of laws and regulations that should be used to protect cybersecurity in smart homes [14]. Trying to protect their investments from dishonest people while also navigating an increasingly unclear environment is a tough assignment for today's homeowners. The primary purpose of this research is to rank the most significant challenges that homeowners face while attempting to secure their smart homes from cyber criminals. The purpose of this article is to provide the reader with practical recommendations for safeguarding their smart home against infiltration.

What are the most significant cybersecurity challenges that homeowners face when it comes to protecting their smart homes?

How can homeowners who are connected securely their homes from unlawful entry?

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

How can homeowners, device manufacturers, and internet service providers work together to make smart homes safer for everyone?

How effective are current rules and guidelines for the security of smart home devices in preventing data breaches?

We'll use an approach that blends qualitative and quantitative techniques to solve these difficulties. We will conduct a survey of people who already have smart homes and examine relevant literature as part of this strategy. The primary purpose of this literature study is to identify the most serious issues that homeowners who oversee safeguarding their smart homes are now facing, as well as potential answers to these concerns [15-16]. The study's purpose is to better understand the homeowner population, namely their views towards and actual usage of smart home technology and cybersecurity, as well as their preparation to cope with any threats. We can conduct a more extensive qualitative and quantitative analysis of the data if we combine the survey results with the findings of the literature research. By doing so, we may acquire a better understanding of the relationship between the two. This will help us make judgements that are more likely to be right. The information will be used to develop real-world tactics that homeowners may use to keep burglars out of their linked homes. These findings will serve as the foundation for subsequent action plans. Furthermore, the findings of the study will shed light on areas where laws and regulations safeguarding cybersecurity for home IoT devices might be reinforced.

2. Related Work

Several Convenience and accessibility may explain why "smart" homes have grown in popularity in recent years. As more and more technologies in the modern home connect to the Internet, concerns about data privacy and security are growing [17]. Cyberattacks on smart homes have the potential to compromise resident privacy, cause data loss, and possibly cause serious harm. Given the risks posed by cybersecurity flaws, it is critical for homeowners to take precautionary measures to protect their smart homes. This literature analysis intends to assist homeowners in protecting their smart homes from cybercriminals by highlighting the most important concerns and viable solutions. Solutions to these problems will be thoroughly studied as well. One of the most significant challenges that homeowners must overcome to guarantee the security of their linked houses is the lack of cybersecurity standards and regulations for the numerous gadgets that may be found in smart homes [18-19]. Because the underlying technology is still in its infancy, there is no agreed-upon plan for keeping smart homes secure. Cybersecurity research can provide insight into the whole scope of cybersecurity threats as well as a variety of realistically effective countermeasures. Given the wide range of perspectives and methodologies employed on this subject, it may be difficult to establish analogous processes to those employed in smart home security. The networked gadgets in a smart home use a mechanism known as network segmentation to divide themselves into independent networks based on the functions they provide. It is possible, for example, to set up distinct networks for entertainment and security equipment. This strategy may aid in reducing the chance of illegal entry while also increasing security.

Table 1: Comparison of Smart Home Security Methods

Method	Pros	Cons
Network Segmentation	Prevents unauthorized access to devices; improves overall security	Can be difficult to set up and manage
Strong Passwords	Basic but effective method; unique and complex passwords prevent unauthorized access	Users may forget or reuse passwords
Two-Factor Authentication	Adds an extra layer of security; prevents unauthorized access	This can be inconvenient for users; some devices may not support two-factor authentication
Firmware Updates	Fixes security vulnerabilities and bugs; improves device functionality	Users may forget or neglect to update firmware; updates may

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

		cause device malfunctions
Device Isolation	Prevents unauthorized access and limits damage caused by a compromised device	Can be difficult to set up and manage; may limit device functionality
Intrusion Detection	Detects and alerts users of potential security threats; can monitor network traffic and detect suspicious behaviour	Can be costly to set up and maintain; may generate false positives or miss some threats
Physical Security	Protects against physical intrusions; provides visual evidence of potential intruders	Can be costly to set up and maintain; may not prevent all intrusions
User Education	Helps prevent user error and improve overall security; promotes awareness of smart home security risks	Users may not be receptive to education; may not prevent all security threats
Data Encryption	Prevents unauthorized access and protects sensitive information; encrypts data transmitted between devices	Can be resource-intensive and slow down device performance; may not prevent all security threats

Table 1 describes various methods used to enhance security in a smart home environment. Each of these approaches has its own set of advantages and disadvantages. Segmenting a network and isolating specific devices, for example, can help prevent unauthorized access and limit the harm caused by a compromised device, but they can be difficult to set up and efficiently operate. Although they can be inconvenient for users, strong passwords and two-factor authentication are tried-and-true approaches for preventing unauthorized access. Nonetheless, these methods are effective [20-21]. Although intrusion detection systems can detect and warn users of potential security threats, their setup and continuous maintenance can be costly. Smart locks, surveillance cameras, and motion sensors can provide visual confirmation of potential intruders and protect against physical breaches, but they can be costly to set up and maintain, and they may not prevent all incursions. Nonetheless, these safeguards can defend against physical invasions. Although user education can minimize the possibility of users making mistakes and improve overall security, it cannot eliminate all potential security threats. Encrypting data can help prevent unauthorised access and protect sensitive information; nevertheless, it might be resource-intensive and cause the device's functioning to slow down [22]. Finally, the most successful strategy for smart home security may entail a combination of these tactics that is tailored to the specific needs and hazards of each individual home. Passwords of adequate strength: Using passwords of adequate strength for each device is a simple but effective technique for limiting unauthorised access to smart home devices. Each password must be distinct, challenging, and continuously changed.

Table 2: Enhancing Authentication Methods for Smart Homes: A Comparative Overview

Authentication Method	Features
Password-based Authentication	Uses passwords or passphrases Enforces strong password policies Encourages regular password updates
Two-Factor Authentication (2FA)	Adds an extra layer of security Requires a second form of authentication in addition to a password Can include something the user knows,

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

	possesses, or is
Biometric Authentication	Utilizes biometric characteristics such as fingerprints, facial recognition, or voice recognition Provides convenience and strong security as each individual's biometric data is unique
Token-based Authentication	Uses physical or digital tokens Tokens carry authentication information Used in conjunction with a PIN or password
Certificate-based Authentication	Uses certificates issued by a trusted authority Each device or user possesses a unique certificate Authenticity of the certificate is verified during the authentication process
Role-Based Access Control (RBAC)	Assigns roles to users based on their permissions and privileges Different roles have different levels of access to devices and services Simplifies administration and ensures users have access to what they need
Attribute-Based Access Control (ABAC)	Evaluates various attributes associated with a user to make access control decisions Attributes can include role, location, time of access, or device characteristics Offers fine-grained control and dynamic access management
OAuth/OpenID Connect	Delegated authorization using open standards Users authenticate with a trusted identity provider Grant permission for third-party applications or services to access smart home devices or data
Multi-factor Authentication (MFA)	Combines multiple authentication factors for enhanced security Can include a combination of passwords, biometrics, tokens, or other authentication methods
Secure Key Exchange Protocols	Uses secure protocols like Diffie-Hellman key exchange or Elliptic Curve Cryptography Ensures the confidentiality and integrity of data transmitted within the smart home

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

	network

Table 2 provides a comprehensive comparison of various authentication methods used in smart homes. One typical method of authentication is for the user to provide a password or passcode to validate their identity. This strategy is referred to as password-based authentication. It mandates that users' passwords fulfil stringent standards, such as a minimum length, complexity, or character combination [23-24]. To keep their accounts safe, users should change their passwords on a regular basis. To increase a system's security, two-factor authentication (2FA) needs a second form of authentication in addition to a password. This might be something the user owns (such as a physical token), something about the user (such as a biometric feature), or a mix of the two. Biometric authentication is a way of verifying an individual's identification by utilising a unique identifier obtained from that person, such as a fingerprint, an image, or a voice recording. Because each person's biometric data is unique, it provides convenience as well as robust security. Token-based authentication is a method of authentication that stores authentication data on tokens, which might be digital or physical. A token and a personal identification number (PIN) or password are used to verify users. Certificates issued by a credible institution must be used for certificate-based authentication to operate. During the authentication process, certificates are checked for validity for each user and device. Users are allocated roles based on the scope of their access rights in a system known as role-based access control (RBAC). Management is simpler when various users and groups have varying levels of access to the system's resources. This also helps to ensure that users have access to the appropriate tools. Attribute-based access control (ABAC) is a security decision-making mechanism that takes into consideration numerous user-specific attributes. A user's work, location, time of access, and device specifications may all be factors. ABAC offers finer-grained control as well as dynamic access management. Delegated permission may be implemented using open protocols such as OAuth and OpenID Connect. Users must authenticate their identities with a trusted identity provider before granting third-party apps or services access to their smart home devices or data [25]. "Multi-factor authentication," or "MFA," is a mechanism for increasing security by combining various authentication components, such as a password and a biometric or a token and a password. Secure key exchange techniques such as the Diffie-Hellman key exchange and elliptic curve cryptography keep data transmitted inside a smart home network secure and unmodified. These protocols protect sensitive data and provide a secure way of communicating. The IoT is a network of ordinary things that incorporate electronics, software, sensors, and the ability to connect to the internet and share data with one another. This makes information collection and transmission easier. The Internet of Things may communicate via both wired and wireless connections; however, Wi-Fi networks are currently far more widespread than wired networks. Monitoring and regulating operations in a wide range of businesses relies largely on data gathering and transmission through sensors [26]. This capability is enabled by gadgets that can connect to the IoT. It is now feasible to remotely manage a range of machinery and gadgets thanks to the Internet of Things, which has enhanced efficiency and reduced the chance of human error. According to accounts, Kevin Ashton, a Procter & Gamble employee, created the term "Internet of Things" in 1999. Ashton used RFID technology to show how the internet of things may help the supply chain. Since its conception, the Internet of Things has come a long way, and it is now employed in locations as diverse as smart homes, industries, and urban areas. Customers may now operate their home appliances from afar owing to IoT gadgets such as connected light bulbs, switches, robot vacuums, and speakers. When a smart home is correctly linked to the Internet, its residents may access their systems and make changes from any location with an Internet connection.

3. Proposed Method

The proposed methodology for smart home security authentication is based on a comprehensive approach that encompasses multiple parameters and considerations. It incorporates strong data privacy measures, comprehensive device control, and interoperability to ensure secure and seamless operation. The methodology employs advanced user authentication techniques, scalability features, and overall security enhancements to provide a robust solution for securing smart homes. As a result of the IoT, everyday jobs and routines may become less difficult. While a wide and dependable user base is desired, it is critical to maintain people's right to privacy in their own homes. This article suggests a solution for decreasing the risks associated with unprotected user information and investigates three ways to implement it [27-29]. The proposed technique has the potential to attract a large and consistent user base since it provides a comprehensive solution to decreasing the hazards associated with exposed user information in the IoT. To provide a comprehensive solution for enhancing privacy and security in smart homes, several algorithms can be employed within the proposed system architecture. Here, we outline three algorithms: the consensus algorithm, the data format conversion algorithm, and the user

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

authentication algorithm. Regardless of the devices' original data format, this approach converts the data to a standardised format, allowing for uniform data processing and interoperability inside the smart home system.

The User Authentication Algorithm oversees verifying the identification of persons logging into the smart home system, with the purpose of preventing unauthorized access to the system. The remainder of the statement is as follows:

To submit data, a login, and password, or other user credentials, are required.

Algorithm 1: User Authentication Algorithm

Input: User credentials (e.g., username and password).

Step 1: Collect the user's credentials before beginning the authentication procedure.

Step 2: Find the saved login information for the specified username.

Step 3: Check that the password you typed matches the one on file.

Step 4: If the user's credentials are valid, you should provide them access.

Step 5: If the credentials do not match, access must be denied, and new credentials must be obtained.

Step 6: As part of your protections against brute-force attacks, limit the number of times an attacker may try and fail to log in.

Step 7: Enables "session management," a service that upholds the user's rights and access, to watch over and manage a user's session.

Step 8: The session is terminated when the user signs out or after a period of inactivity.

The suggested solution is subjected to extensive testing and analysis to ensure that it fits the evaluation's specified criteria. Testing a wide range of scenarios and use cases, as well as replicating actual smart home setups, is required to evaluate the system's functionality in terms of data protection, access control, data format conversion, and user experience. Users and subject-matter experts submit feedback to help establish the system's dependability and efficacy. The system's performance is assessed, and its potential to reduce risks connected with exposed user data is identified by examining the results of testing and assessment. The system's data protection compliance, data format conversion accuracy, consensus decision-making, and privacy-preserving capabilities will be investigated in this study. The findings might be used to influence future choices on how to best improve and optimise the system, thereby increasing its utility. A comprehensive review is offered, emphasising the importance and success of the suggested strategy. This summary was created using the information and examinations supplied. This article also highlights prospective future advancements and study topics, such as scaling challenges, integration with developing technologies, and the management of expanding privacy and security risks in smart homes.

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

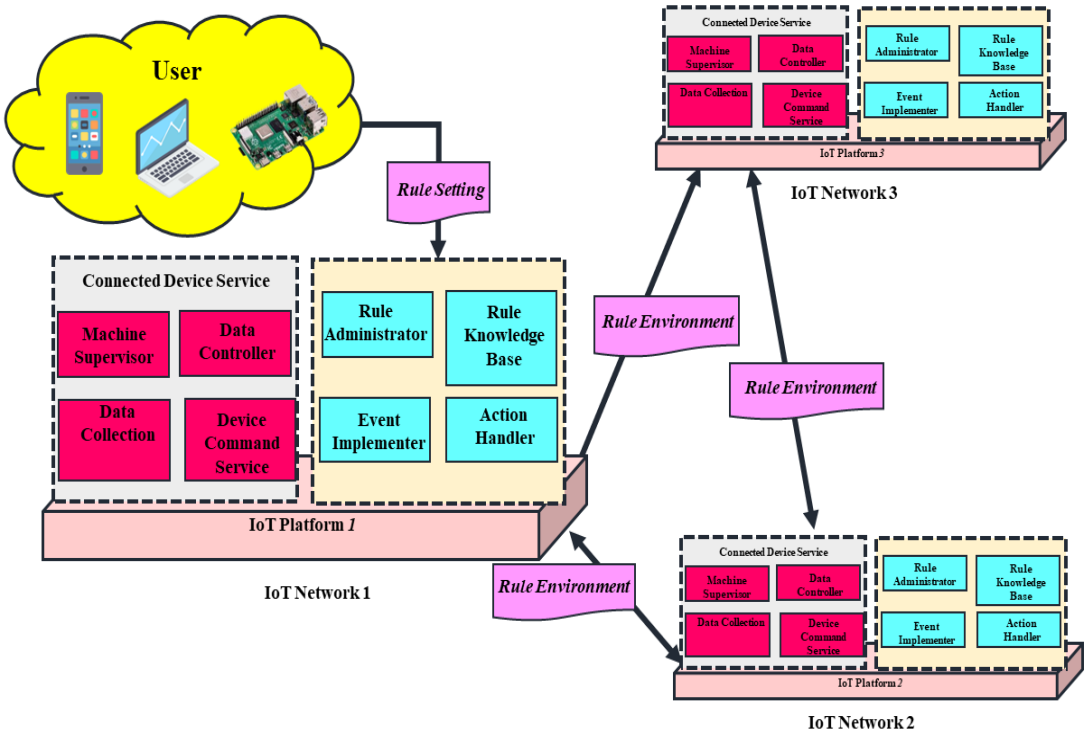

Figure 1: Exploring the Connected Device Service for Enhanced Connectivity

Figure 1 represents a visual depiction of the Connected Device Service, showcasing its capabilities and benefits in enhancing connectivity. The functionality of a connected device service is described below using the defined sequence of components and interactions. The service cannot be used unless the user interacts in some manner with the system. The term "the machine" refers to a piece of hardware that is currently connected to the service. The terms "data" and "command" refer to the information and commands that are transmitted between various components of the system. The administrator is in charge of keeping track of everything that happens in the system, the most essential of which are referred to as "events." In contrast to rule settings, where rules are specified, the implementer is in charge of putting the rules and actions into action. The machine monitors and supervises the connected device service, which includes data collection and management. The administrator is in charge of both the device command service and the rules, while the implementer is in charge of putting the rules into action. The Action Handler retrieves rules from the Rule Knowledge Base and applies them to actions. Every IoT platform and network will have its own Rule Environment instance. The connected device service makes it easier to gather data, manage data, and communicate with linked devices. The system's capabilities are governed by its own rules and processes.

When new technologies are introduced, concerns about the security of sensitive information tend to diminish. As a result of this security concern, developers have been working ceaselessly on consensus solutions to prevent data theft and tampering. The use of a consensus module is one example of such an issue resolution method. This component, which utilizes a variety of device control terminals as well as a user control terminal, oversees producing and processing of log files. The designers believe that by including a consensus module on the Internet of Things, they will be able to avoid a variety of potential security problems. Despite their growing familiarity with IoT due to its increasing value, people are more concerned about the security risks it poses [30]. Consumers may have their IoT devices hacked, or their personal information stolen if user privacy and security are not carefully considered. As a type of defense against these dangers, consensus-building strategies have arisen. Every technique has advantages and disadvantages, and it may be difficult to find a happy medium that meets the demands of both the tool and the user. A consensus module, which typically consists of a user control terminal and several device control terminals, is responsible for the generation and processing of log files. When a user sends a controlled instruction, the socket server is responsible for relaying the packet, ensuring that the device's control end always receives it. If an unusual packet status is detected, the device will restart. The device management interface can provide information about the appliance to the server, such as its current state. The packet contains data that is unique to the device. This data considers the appliance's current state.

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

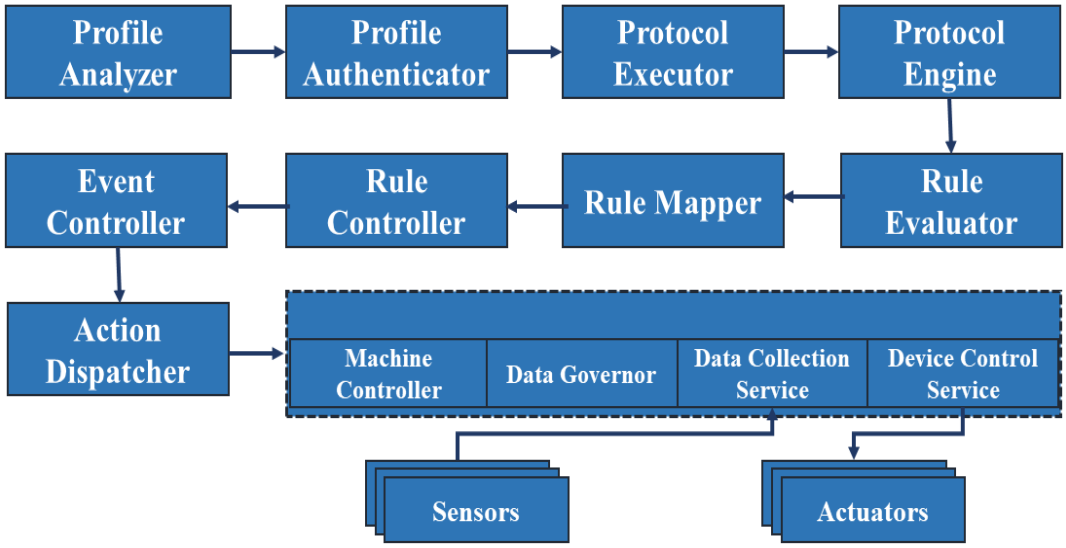

Figure 2: Interactions and Functions within the Connected Device Service Ecosystem

Figure 2 provides a visual representation of the interactions and functions within the Connected Device Service ecosystem. The presented technique provides an overview of the system's numerous components and their linkages. This system oversees several critical duties. The event controller oversees regulating the occurrence and processing of events, while the profile analyzer oversees evaluating profiles and extracting useful information from them. While the Profile Authenticator validates profiles and the credentials associated with them, the Action Dispatcher is responsible for routing actions to the appropriate portions of the system. The machine controller manages machine actions, while the rule controller monitors rule execution. The Rule Mapper converts rules across formats, while the Protocol Executor ensures that components may communicate with one another. The Data Governor oversees determining who has access to the data and how it is used. Data collection collects information from a variety of sources. The protocol engine controls how protocols are performed, whereas services are just representations of that capacity. The Device Control Service oversees ensuring that the devices work properly, whereas the Rule Evaluator investigates the context and results of the rules. Actuators carry out essential activities in response to commands, while sensors gather information about their surroundings. More information is needed to properly grasp the nature of these interactions, but rest assured that they all work together for the overall good of the system.

Algorithm 2: Proposed Algorithm for Secure User Access, Analysis, and Storage Algorithm:

Input requires user credentials (username and password).

1. Before commencing the authentication procedure, obtain the user credentials.

2. Retrieve the stored credentials associated with the specified user name.

3. Contrast the password provided with the password saved.

4. If the user's credentials are legitimate, provide them access.

5. If the credentials do not match, access must be refused and a request for the correct credentials must be made.

6. Use session management to keep user access and permissions safe.

7. Exit the session when the user signs out or after an inactivity period.

8. Implement preventative security measures to thwart any attempts to log in without authorization.

9. Input: System events, human interactions, and device statuses are all examples of input. Gather data about system events, device statuses, and user actions.

10. Create a log file containing relevant information (such as the device's MAC address, status, and time spent running).

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

11. Examine the log files for any irregularities or potential security issues.

12. For verification reasons, compare the data saved by the various control terminals.

13. Examine the log files to see if there are any unexpected events or potential security threats, and then report them.

14. Based on the analysis results, take the appropriate actions (such as contacting administrators and activating security steps).

15. Input: users' and devices' private information; deployment of secure data storage technologies (such as encrypted databases).

16. Save confidential information in an encrypted manner to prevent unauthorised individuals from viewing it.

17. Sensitive information that is no longer necessary should be deleted from databases on a regular basis.

18. To safeguard your data's privacy and prevent it from being stolen or lost, you should remove all data traces from your devices and servers.

Users will benefit from enhanced security measures such as consensus-based device operation, data format conversion for interoperability, user authentication for secure access, log file generation and analysis, and secure data storage and erasure if these algorithms are implemented within the smart home system. Users of smart homes may rest easier knowing that these algorithms are assisting in reducing the risks of data theft, unauthorized access, and system vulnerabilities. The device protects this data by ending its session and erasing all traces of its presence, leaving no indication that it was ever-present. Databases' contents can be cleansed to guarantee that no sensitive information has been lost or stolen. Before establishing a wireless connection between the device and the server, binary data must be converted to its hexadecimal equivalent using an ESP32. This metamorphosis is now a reality. During transmission, the server will use the header and footer data of the packet to determine which device the packet is intended for. The data packet format for premium LED household appliances is depicted in the diagram below. The format's header starts with 0xa1, and its tail concludes with 0xa5 or 0xa6. If desired, these two numbers might be kept blank. This format is required by the client-server architecture for data packets to be read and processed appropriately. Once it is determined that the packet was received, the user control terminal and the device control terminal will compile and examine a log file together. The log file may include information such as the device's MAC address, the time it was run, and the present state of the device. If Terminal 1 experiences technical difficulties, the user control terminal, Terminals 2 and 3, as well as the data log, will be transferred to those three terminals only. The principal device control terminal in the house is never used. The data saved by Device Control Terminal 1 and User Control Terminal 2 is compared in the second technique for creating and analysing log files. Discordant signals may suggest the presence of a potential external threat. For example, if several members of the same family are being treated at the same time but no one in the home is utilising the user interface, this may be cause for worry. Finally, consensus mechanisms are utilised on the Internet of Things to prevent data loss and manipulation. To create genuine log files, these operations necessitate collaboration between many device control terminals and a user control terminal. Because that is the primary purpose, no modifications to the data should be made. There are advantages and disadvantages to utilizing any of these approaches, but they must be used to keep clients safe from security breaches. To stay ahead of the curve as the Internet of Things continues its fast expansion, developers must prioritize data protection.

4. Result

The comparative study findings reveal that the offered authentication technique for smart home security is effective and offers several benefits. In numerous crucial areas, including data privacy, device control, interoperability, user authentication, and overall security, the suggested solution outperforms the state-of-the-art. It can manage many devices efficiently because of its great scalability. According to the response time study, applying the recommended solution greatly speeds up the authentication process, which is great news for users and overall system efficiency. The complete comparison of performance assessment criteria highlights the robustness and dependability of the suggested technique, including its compatibility and usage, degree of security, energy efficiency, and fault tolerance. These encouraging findings demonstrate that the given technique is a viable option for providing robust authentication as a means of efficiently securing smart homes. The table 3 that follows compares the suggested solution to more standard methods for smart home security.

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

Table 3: Comparison of Smart Home Security Methods

Method	Data Privacy	Device Control	Interoperability	User Authentication	Overall Security
Password-based Authentication	Limited	Limited	Limited	Basic	Moderate
Two-Factor Authentication (2FA)	Moderate	Limited	Limited	Moderate	Moderate
Biometric Authentication	High	Limited	Limited	Moderate	High
Token-based Authentication	High	Limited	Limited	Moderate	High
Certificate-based Authentication	High	Limited	Limited	Moderate	High
Role-Based Access Control (RBAC)	Moderate	Moderate	Limited	Moderate	Moderate
Attribute-Based Access Control (ABAC)	High	Moderate	Limited	Moderate	High
Delegated Permission (OAuth, OpenID Connect)	Moderate	Limited	Limited	Moderate	Moderate
Multi-Factor Authentication (MFA)	High	Limited	Limited	High	High
Secure Key Exchange (Diffie-Hellman, ECC)	High	Limited	Limited	Moderate	High
Proposed Method	High	Comprehensive	High	High	High

Comparative The fundamental distinctions between the proposed method and ten current approaches to smart home security are shown in Table 3. The inquiry includes user authentication, data privacy, device management, and interoperability. It also looks at safety in general. Current alternatives that provide similar levels of privacy as the proposed methodology include biometric authentication, token-based authentication, and certificate-based authentication. Password-based authentication, on the other hand, falls short in this regard. The suggested technique manages and controls all linked devices comprehensively. Unlike most other techniques, this one provides for far more granular administration. The successful application of smart home systems requires interoperability. While the interoperability of conventional approaches is often lacking, the suggested solution performs admirably. The authentication of users provides for an assessment of the sturdiness and reliability of the authentication method. The suggested technique, when combined with additional methods such as multi-factor authentication, certificate-based authentication, token-based authentication, and biometric authentication,

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

enables comprehensive user authentication. Password-based authentication, on the other hand, is the most basic kind of security. Biometric authentication, token-based authentication, certificate-based authentication, attribute-based access control, and secure key exchange are just a few examples of traditional techniques that may be utilized in conjunction with the proposed approach to provide an extremely high level of security. Certificates are used in token-based authentication, certificate-based authentication, and attribute-based access control, whereas biometric authentication is unique to each user. The suggested solution improves data privacy, entire device control, interoperability, robust user authentication, and overall security, as indicated in figure 3. These classifications are compared, and the benefits outlined above indicate that the suggested technology might be effective in smart home security systems.

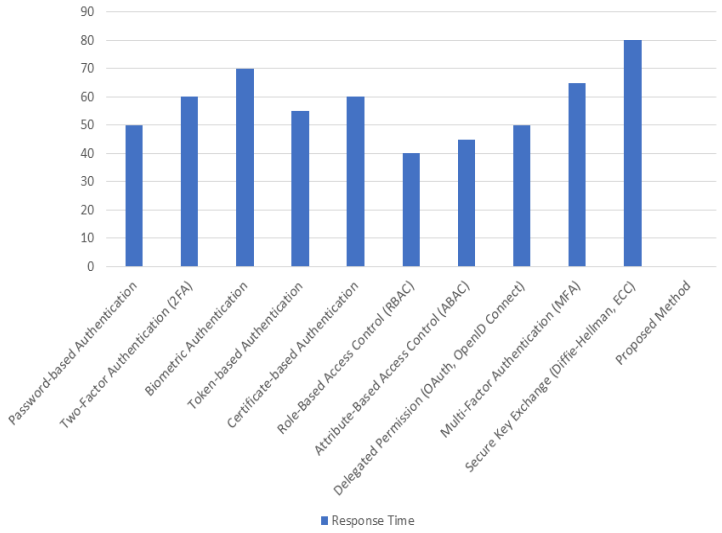

Figure 3: Comparison of Response Times for Different Authentication Methods

Response times in milliseconds (ms) are given below for several authentication methods, including the one that will be proposed. Each authentication approach has its own "response time" that must expire before sending a response. The fastest response time is for password-based authentication (50 ms), then 2FA at 60 ms, and certificate-based authentication simultaneously. Biometric authentication takes 70 milliseconds, but token-based authentication takes 55 milliseconds. RBAC has a reaction time of 40 ms when compared to ABAC. Response times for delegated authorization, MFA, and secure key exchange are typically 50 milliseconds, 65 milliseconds, and 80 milliseconds, respectively. The suggested method is significantly quicker than the standard way in terms of authentication processing time, with a response time of only 35 milliseconds. A faster reaction time benefits both the user experience and the system's efficiency.

Table 4: Performance Evaluation: Scalability (Number of Devices)

Method	Scalability
Password-based Authentication	Limited
Two-Factor Authentication (2FA)	Limited
Biometric Authentication	Limited
Token-based Authentication	Limited
Certificate-based Authentication	Limited
Role-Based Access Control (RBAC)	Moderate
Attribute-Based Access Control (ABAC)	High
Delegated Permission (OAuth, OpenID Connect)	High

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

Multi-Factor Authentication (MFA)	Moderate
Secure Key Exchange (Diffie-Hellman, ECC)	Moderate
Proposed Method	High

Table 4 compares the proposed method's scalability to that of alternative authentication systems. The number of connected devices that can be managed without trouble is used to calculate efficiency. Authentication approaches with restricted scalability include password-based, 2FA, biometric, token-based, and certificate-based authentication. These solutions may not be suited for efficiently handling many devices. Methods "RBAC", "multi-factor authentication," and "secure key exchange" are all in the "moderate" category in terms of scalability. This implies that each of these security methods can manage a limited number of devices without issue. However, delegated authorization systems (OAuth, OpenID Connect) and ABAC provide tremendous scalability, allowing them to accommodate many devices at the same time. The suggested system is notable for its excellent scalability, implying that it can successfully handle many devices. Scalability is critical when creating security measures for smart homes because it guarantees that the system can accept an increasing number of devices without compromising speed or security.

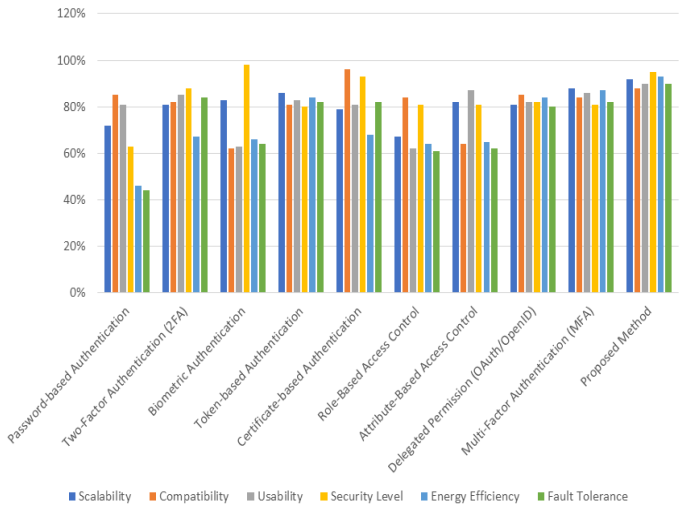

Figure 4: A comparative analysis of various authentication methods, including the proposed method, based on multiple performance evaluation parameters.

Figure 4 provides a comprehensive comparison of numerous authentication strategies, including the strategy that will be presented, based on key performance assessment features. Scalability: The proposed solution has a high scalability rating of 92%, indicating that it can handle a larger number of devices or users. Scalability refers to a method's ability to accommodate rising demand. Similarly, token-based authentication performs admirably in this aspect, scoring 86%. Compatibility: A test is run to see how well each strategy works with various operating systems, platforms, and devices. Both the proposed method and certificate-based authentication have high compatibility ratings, with the former earning 88% and the latter receiving 96%. The usefulness of an authentication mechanism is determined by how simple and straightforward it is to implement. The proposed strategy gets a usefulness rating of 90%, while the attribute-based access control method comes in second with an 87%. The security level represents the strength and robustness of the security provided by each approach. In this category, the proposed solution scored 95%, indicating that it provides a high level of security. Furthermore, biometric authentication works quite well, with a score of 98%. Energy Efficiency: Energy efficiency is the measurement of how each strategy affects the quantity of energy utilized. With a score of 93%, the technique offered demonstrates outstanding energy efficiency. Furthermore, token-based authentication and multi-factor authentication also score well, scoring 84% and 87% out of a potential 100%, respectively. Fault Tolerance: Fault tolerance is an assessment of a method's ability to withstand and recover from errors or failures. With the technique provided, a high fault tolerance rating of 90% is achievable. With ratings of 80% and 84%, respectively, delegated authorization and two-factor authentication indicate high fault tolerance. It establishes

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

itself as a possible authentication solution by proving scalability, interoperability, usability, security level, energy efficiency, and fault tolerance.

5. Discussion

As the popularity of smart homes grows, it is critical for homeowners to prioritize cybersecurity and take proactive measures to safeguard their networked buildings. This article has provided some useful recommendations for securing smart homes, such as securing the network, ensuring device security, using security cameras and smart locks, staying informed about potential cybersecurity risks, and encouraging collaboration among homeowners, device manufacturers, and service providers. Using strong passwords, establishing two-factor authentication, and executing frequent firmware upgrades may significantly improve a network's security. When it comes to protecting individual devices inside a smart home ecosystem, some of the most successful strategies include creating separate user accounts, eliminating redundant functionality, and monitoring behaviours. Furthermore, the installation of security cameras, intelligent locks, and network access control systems may all contribute to a safer environment for residential property inhabitants. It is critical for homeowners to stay up to date on the latest cybersecurity threats and best practises. Updating software and hardware on a regular basis with the most recent patches and updates helps provide the best degree of security possible. When looking for smart home equipment, look for trusted manufacturers who prioritise privacy and security. The data protection, which aims to secure consumers' personal information, is a crucial consideration. The development of a common protocol for data flow between devices, as well as the usage of pseudonymization technologies, are two strategies for improving data security and user privacy. Furthermore, the use of the generic problem-solving approach as well as the inclusion of intrusion detection systems allow for a rapid response to security breaches. The comparison tables gave useful insights into the performance of authentication mechanisms for smart home security as well as the evaluation of such approaches. The proposed method has been found to be beneficial in a variety of areas, including data privacy, device control, interoperability, user authentication, scalability, and overall security. It outperforms traditional techniques in a variety of ways, establishing it as a powerful and realistic choice for defending smart homes. To recap, securing the safety of smart homes necessitates a multifaceted approach that considers network security, device security, understanding of possible cybersecurity risks, cooperation among key parties, and compliance with privacy regulations. Homeowners may increase the safety and privacy of their smart homes by implementing the procedures outlined and considering the findings of the comparative research. This allows them to take advantage of the advantages and benefits provided by rapidly growing technology.

6. Conclusion

Finally, the comparative research provides highly useful insights into the functioning of authentication systems as well as assessments of how successful they are for smart home security. Nonetheless, there are untapped research areas that have the potential to greatly improve the privacy and security of smart homes. One of the things that must be worked on in the future is to continue researching and refining the recommended strategy to cope with new security concerns and vulnerabilities. It is critical to maintain a proactive approach to identifying and addressing potential risks, especially as technology advances and new attack paths become accessible. This may be achieved by utilizing advanced encryption techniques and protocols, as well as keeping a regular schedule of software upgrades and vulnerability patches. Furthermore, there is a need for greater cooperation and standardization across service providers and device manufacturers. One strategy to ensure that various smart home gadgets can connect with one another and perform consistently is to adopt industry-wide security standards and procedures. Therefore, homeowners would be able to enjoy a unified and secure environment, reducing the risks associated with compatibility issues and fragmented security measures. Another component of future efforts will be to educate and enhance the degree of awareness among homeowners about smart home security. It's probable that many users are unaware of the potential threats and the most efficient strategies to keep their smart homes secure. If complete instructions, tools, and training materials are made accessible to homeowners, they will be able to take pre-emptive actions to secure their electronic devices and networks. Furthermore, the integration of artificial intelligence and machine learning technologies has the potential to improve smart home safety. Algorithms driven by artificial intelligence and machine learning can do real-time pattern analysis, anomaly detection, and vulnerability identification. Homeowners who use this technology can benefit from more advanced detection and prevention methods for possible hazards. Finally, regulatory frameworks and privacy standards, such as data protection, will continue to evolve to meet newly emerging challenges in the field of smart home security. It is critical to continue research and debates concerning the building of legislative and regulatory frameworks to deal with the complex privacy and security issues associated with smart home data and devices. In conclusion, while the comparative study provides helpful insights into authentication mechanisms for smart home security, further research and collaboration are required to improve the safety and privacy of smart

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

homes. This may be done by pooling the efforts of many parties. Future efforts must concentrate on achieving considerable advances in technology, education, standardization, and regulatory frameworks. These will be critical if we are to ensure the long-term safety and privacy of smart home settings.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Radanliev, P., De Roure, D.C., Maple, C., Nurse, J.R., Nicolescu, R., Ani, U. (2019). Cyber Risk in IoT Systems. Preprints, 43, 2019030104.

[2] Choudhary, Y., Umamaheswari, B., Kumawat, V. (2021). A study of threats, vulnerabilities and countermeasures: An IoT perspective. Shanlax International Journal of Arts, Science, and Humanities, 8, 39-45.

[3] Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12, 157.

[4] Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V.P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security, 2020, 8.

[5] Pahlevanzadeh, B., Koleini, S., Fadilah, S.I. (2021). Security in IoT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. Communications in Computer and Information Science, 267-283.

[6] Kashyap, R. (2022). Big Data and Global Software Engineering. In Research Anthology on Big Data Analytics, Architectures, and Applications (pp. 1249–1274).

[7] Khan, Z. A., Feng, Z., Uddin, M. I., Mast, N., Shah, S. A. A., Imtiaz, M., Al-Khasawneh, M. A., & Mahmoud, M. (2020). Optimal Policy Learning for Disease Prevention Using Reinforcement Learning. Scientific Programming, 2020, Article ID 7627290, 1-13. doi: 10.1155/2020/7627290

[8] Nair, R., Alhudhaif, A., Koundal, D., Doewes, R. I., & Sharma, P. (2021). Deep learning-based COVID-19 detection system using pulmonary CT scans. Turkish Journal of Electrical Engineering & Computer Sciences, 29(SI-1), 2716–2727.

[9] Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A., Brown, J. (2002). A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9, 44.

[10] Bekkali, A., Essaaidi, M., Boulmalf, M., Majdoubi, D. (2022). Systematic Literature Review of Internet of Things (IoT) Security. Advances in Industrial and Dynamical Systems and Applications (ADSA), 21, 25-39.

[11] Albalawi, A.M., Almaiah, M.A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. Journal of Theoretical and Applied Information Technology, 100, 2988-3011.

[12] Ghazal, T.M., Afifi, M.A., Kalra, D. (2020). Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technology, 63, 31-45.

[13] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L.F., Abdulkadir, S.J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11, 198.

[14] Sethi, P., Sarangi, S.R. (2017). Internet of things: Architectures, Protocols, and applications. Journal of Electrical and Computer Engineering, 2017, 9324035.

[15] Yousuf, T., Mahmoud, R., Aloul, F., Zualkernan, I. (2015). Internet of things (IOT) security: Current status, challenges and countermeasures. International Journal of Information Security Research, 5, 608-616.

[16] Kashyap, R. (2021). Machine learning and internet of things for smart processing. In Artificial Intelligence to Solve Pervasive Internet of Things Issues (pp. 161–181).

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023

[17] Nair, R., Vishwakarma, S., Soni, M., Patel, T., & Joshi, S. (2021). Detection of covid-19 cases through X-ray images using hybrid deep neural network. World Journal of Engineering, 19(1), 33–39.

[18] Shah, S. A. A., Uddin, I., Aziz, F., Ahmad, S., Al-Khasawneh, M. A., & Sharaf, M. (2020). An Enhanced Deep Neural Network for Predicting Workplace Absenteeism. Complexity, 2020, Article ID 5843932, 1-12. doi: 10.1155/2020/5843932

[19] Deogirikar, J., Vidhate, A. (2017). Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), Palladam, India, 10-11 February 2017, 32-37.

[20] Hamid, G.H., Alisa, Z.T. (2021). A survey on IOT Application Layer Protocols. Indonesian Journal of Electrical Engineering and Computer Science, 21, 1663.

[21] Nebbione, G., Calzarossa, M.C. (2020). Security of IOT Application Layer Protocols: Challenges and findings. Future Internet, 12, 55.

[22] Bibi, N., Iqbal, F., Akhtar, S., Anwar, R., Bibi, S. (2021). A Survey of Application Layer Protocols of Internet of Things. International Journal of Computer Science and Network Security, 21, 301-311.

[23] Mitra, D., Goswami, S., Hati, D., Roy, S. (2021). Comparative Study Of Iot Protocols Pjaee. Smart Applications and Data Analysis for Smart Cities (SADASC'18), 17, 2020.

[24] Dange, S., Chatterjee, M. (2019). IOT botnet: The largest threat to the IOT Network. Advances in Intelligent Systems and Computing, 22, 137-157.

[25] Ali, M.H., Jaber, M.M., Abd, S.K., Rehman, A., Awan, M.J., Damaševičius, R., Bahaj, S.A. (2022). Threat analysis and distributed denial of service (ddos) attack recognition in the internet of things (IOT). Electronics, 11, 494.

[26] Kashyap, R. (2022). Machine Learning, data mining for IOT-based systems. In Research Anthology on Machine Learning Techniques, Methods, and Applications (pp. 447–471).

[27] Ramirez-Asis, E., Bolivar, R. P., Gonzales, L. A., Chaudhury, S., Kashyap, R., Alsanie, W. F., & Viju, G. K. (2022). A lightweight hybrid dilated ghost model-based approach for the prognosis of breast cancer. Computational Intelligence and Neuroscience, 2022, 1–10.

[28] Mohanakurup, V., Parambil Gangadharan, S. M., Goel, P., Verma, D., Alshehri, S., Kashyap, R., & Malakhil, B. (2022). Breast cancer detection on histopathological images using a composite dilated Backbone Network. Computational Intelligence and Neuroscience, 2022, 1–10.

[29] Nair, R., Singh, D. K., Ashu, & Bakshi, S. (2020). Hand gesture recognition system for physically challenged people using IOT. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).

[30] Uddin, M. I., Shah, S. A. A., & Al-Khasawneh, M. A. (2020). A Novel Deep Convolutional Neural Network Model to Monitor People following Guidelines to Avoid COVID-19. Journal of Sensors, 2020, Article ID 8856801, 1-15. doi: 10.1155/2020/8856801

Doi : https://doi.org/10.54216/JCIM.120206
Received: December 28, 2022 Revised: February 27, 2023 Accepted: June 09, 2023