

Mitigating Security Challenges in the Convergence of Internet of Things and Cloud Computing: A Comprehensive Research Study

¹Tejaskumar B. Modi, ²Dr. Himanshu N. Patel and ³Dr. Nilesh K. Modi

¹Assistant Professor, Kalol Institute of Management (MCA), Kalol, Gujarat, India.

²Assistant Professor, Department of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat, India.

³Professor and Director, Department of Computer Science, Dr. Babasaheb Ambedkar Open University, Ahmedabad, Gujarat, India.

ARTICLE DETAILS

Article History

Published Online: 20 August 2021

Keywords

Internet of Things (IoT), Cloud Computing, Security Challenges, Cryptographic Techniques, Threat Detection

*Corresponding Author

Email proftejasmodi@gmail.com

ABSTRACT

Healthcare, transportation, and smart cities are just a few of the fields that stand to benefit greatly from the combination of IoT and cloud computing. However, many new security threats have emerged as a result of this convergence, necessitating thorough analysis and effective countermeasures. This study provides valuable insights into the developing threat environment, cryptographic approaches, identity and access management, secure communication, and threat detection that arise from the merging of IoT and cloud technologies. This research investigates the efficiency of security procedures and standards developed specifically for this convergence. Case studies and recommendations based on actual deployments are provided as examples of how to implement secure practises. In addition, it investigates the potential of cutting-edge security technologies like blockchain and AI. Since following data protection standards is crucial in the current environment, we also discuss concerns related to regulatory compliance and privacy. This article finishes by stressing the need for constant vigilance in the face of security threats, and it offers guidelines and suggestions to help make the confluence of the Internet of Things and the cloud a safer place. Securing this convergence is not a luxury but a necessity in light of the continuing exponential rise of IoT and the centrality of cloud computing to contemporary computing.

1. Introduction

A new age of technical advancement and interconnectedness has arrived with the advent of the Internet of Things (IoT) and the widespread use of cloud computing. While these two revolutionary paradigms have different purposes and origins, they are converging at a pivotal juncture that promises unparalleled data-driven insights, efficiency advantages, and ease across a wide range of industries. This introduction starts by describing both the Internet of Things and cloud computing independently, elaborating on the features and benefits of each. The importance of their merging is then emphasised, along with the far-reaching effects on industry and society at large that will result. The term "Internet of Things" (IoT) is used to describe a system in which everyday things are linked to one another and to other devices and systems online so that they may gather and share data. Smartphones, wearable devices, industrial machinery, and commonplace home appliances are just a few examples of the enormous range of things that fall under the umbrella term "smart" or "connected" technologies. Massive volumes of data are produced by IoT gadgets, fostering a system in which the real and virtual worlds interact in natural ways.

However, cloud computing is a concept for providing on-demand network access to a shared pool of configurable computing resources such as servers, storage, databases, networking, software, and analytics. To supplement their in-house hardware

and software, businesses and people are increasingly turning to cloud services. The easiness with which applications and data may be deployed and managed is enhanced by the services' scalability, adaptability, and low cost. An important crossroads in the development of technology is being reached with the coming together of the Internet of Things and cloud computing. Together, the cloud's huge computing power and storage capacity for data analysis, processing, and storage is combined with the capabilities of IoT devices, which are skilled at detecting and collecting data from the real world. Real-time data analytics, remote monitoring, predictive maintenance, and autonomous decision-making are just some of the possibilities that may be realised as a result of this convergence.

2. Security Threat Landscape

As the Internet of Things (IoT) and cloud computing continue to converge, new security threats have emerged, making it more important than ever to take a diligent and flexible approach to protecting data and systems in the cloud. In this article, we'll look at the many security concerns plaguing IoT and cloud infrastructures, as well as the most frequent vulnerabilities targeted by cybercriminals.

2.1 Types of Security Threats in IoT and Cloud Environments

Data Breaches: Data breaches are a constant danger in the Internet of Things and cloud computing environments. Threat

actors aim to get unauthorised access to sensitive data, including personal information, intellectual property, and other proprietary information.

Malware and Ransomware: Data theft, system compromise, and ransomware attacks in which data is encrypted and held hostage may all result from malicious software infecting IoT devices or cloud infrastructure.

Distributed Denial of Service (DDoS) Attacks: IoT devices and cloud servers are vulnerable to Distributed Denial of Service (DDoS) assaults, which flood their systems with so much data that they crash. Losses in productivity and money may result from these kinds of assaults (Yu et al., 2019).

Man-in-the-Middle (MitM) Attacks: Attackers in the Internet of Things may perform Man-in-the-Middle (MitM) attacks by snooping on communications between endpoints and the cloud and changing or erasing data (Sicari et al., 2015).

Device Tampering: Attackers may get access to systems by physical tampering or unauthorised modification of IoT devices, jeopardising their functioning and integrity.

2.2 Common Vulnerabilities

Weak Authentication: Many Internet of Things devices and cloud services use default or otherwise insecure authentication techniques (Alaba et al., 2017).

Inadequate Encryption: Sensitive data may be intercepted if just partially encrypted. Information security encompasses safeguarding data at both its source and its destination (Santos et al., 2018).

Lack of Patch Management: Known vulnerabilities in IoT devices typically go untreated because of a lack of patch management (Gupta et al., 2018).

Insecure APIs: Attackers may take advantage of poorly protected APIs in cloud services in order to change or steal data (Sun et al., 2017).

Device and Network Misconfigurations: Misconfigurations in the network or on the device itself might leave an organisation vulnerable to cyber-attacks. Misconfigurations may allow unauthorised access to systems or the disclosure of sensitive data (Zhang et al., 2019).

It is crucial to have a multi-layered security strategy that includes network protection, data encryption, access limits, and constant monitoring in order to deal with these security risks and flaws. To cope with the ever-changing nature of the threats plaguing IoT and cloud infrastructures, constant vigilance and proactive security measures are required.

3. Security Challenges in IoT and Cloud Convergence

The Internet of Things (IoT) and cloud computing are converging, creating a potentially fruitful environment for innovation but also one riddled with complex security risks. To protect the privacy, security, and reliability of information and services, these obstacles must be overcome. Important security issues are discussed here:

3.1. Data Privacy and Confidentiality Concerns: Large volumes of private information are created, communicated, and stored when IoT and cloud services combine. There are serious worries about the privacy and security of personal information because of this. Access to confidential material without permission may lead to privacy breaches, legal ramifications, and damaged reputations (Khan, Salah, & Almaini, 2018). Encrypting data, keeping it safe, and following privacy laws are all crucial.

3.2. Authentication and Authorization Issues: Authentication and authorisation systems are crucial parts of IoT and cloud environment security, yet they are often overlooked. Due to their typically meagre processing power, IoT devices may make strong authentication difficult. Maintaining usefulness while restricting access to just authorised parties is a challenging problem (Al-Fuqaha et al., 2015). Building reliable methods for user identification and access control is essential.

3.3. Data Integrity and Trustworthiness: Reliability and trustworthiness of data are essential for preventing accidental or malicious changes to information while it is in motion or stored. Data reliability is particularly important in safety- and mission-critical decision-making applications (Ray et al., 2018). Data integrity may be checked with the use of cryptographic hashing and digital signatures.

3.4. Scalability and Resource Constraints in IoT Devices: Many IoT devices have restricted processing and storage capabilities. To get around these limitations, security solutions need to be resource-efficient (Raza et al., 2019). Scalability and resource constraints may be reduced by using lightweight encryption techniques, optimised communication protocols, and effective security upgrades.

3.5. Insider Threats and External Attacks: The increased attack surface caused by the combination of IoT and cloud settings leaves systems vulnerable to both internal and external assaults. IoT device and cloud infrastructure access may be abused by malicious insiders (Ghose, Acquisti, & Telang, 2016). Vulnerabilities, meantime, may be exploited by external attackers to obtain unauthorised access, conduct DDoS assaults, or compromise data. To reduce these dangers, you need a reliable intrusion detection system, constant monitoring, and well-trained staff.

Convergence of IoT and cloud computing presents complex and ever-evolving security issues. In order to overcome these obstacles, a comprehensive strategy that takes into account technological measures, regulatory conformity, and user awareness is required. To guarantee the smooth and safe functioning of IoT and cloud systems, collaboration between stakeholders and continual research in security solutions are essential.

4. Security Protocols and Standards

The confluence of the Internet of Things (IoT) and cloud computing places an increased emphasis on the need of security protocols and standards in protecting the integrity, confidentiality, and availability of data. This part introduces the reader to the many security protocols now in use, describes the

significance of such standards as MQTT, CoAP, and OAuth, and assesses the efficacy of each in protecting the Internet of Things and the cloud.

4.1 Overview of Existing Security Protocols

Communication and data sharing between devices and systems can only be made safe via the use of security protocols, which are predetermined sets of rules and processes. Convergence of the Internet of Things and the cloud has led to widespread adoption of numerous well-established security protocols:

Transport Layer Security (TLS): Data in transit is encrypted by Transport Layer Security (TLS), which guarantees safe communication. It ensures the privacy, security, and authenticity of your data (Rescorla, 2008).

Secure Shell (SSH): SSH is used for safe remote access to cloud servers and Internet of Things devices. This system employs cryptography for message authentication and encryption.

IPsec (Internet Protocol Security): Internet Protocol Security (IPsec) is a method for encrypting data sent across a network's Internet Protocol (IP) layer. It may be used to protect connections between Internet of Things devices and cloud services by creating an encrypted tunnel for data transfer (Kent & Seo, 2005).

4.2 Standards such as MQTT, CoAP, and OAuth

To meet the special protection needs of IoT and cloud settings, many standards have evolved:

MQTT (Message Queuing Telemetry Transport): The Message Queuing Telemetry Transport, or MQTT, is a simple publish-subscribe protocol used for exchanging data between devices in the Internet of Things. Authentication and data encryption are also supported, making it a good choice for use in safe IoT connections.

CoAP (Constrained Application Protocol): The Constrained Application Protocol (CoAP) was developed with low-power Internet of Things gadgets in mind. Features for protecting data in transit, such as Datagram Transport Layer Security (DTLS), are included.

OAuth (Open Authorization): OAuth (Open authorisation) is a popular authorisation protocol that hides user credentials while yet allowing access to restricted resources. IoT and cloud service security relies heavily on it.

4.3 Evaluating Their Effectiveness

Implementation, configuration, and use case all have a role in whether or not security protocols and standards for the internet of things and the cloud are successful. For an analysis of their efficacy:

Threat Model Analysis: Analysing the threat model may help you evaluate the security of your Internet of Things (IoT) and cloud applications. To counteract unique risks, unique security measures must be implemented.

Scalability and Resource Efficiency: Examine how well protocols and standards scale and how effectively they use resources in low-powered IoT devices. Shelby and Hartke (2014) state that under limited resources, lightweight protocols like as MQTT and CoAP are preferred.

Compliance and Interoperability: The capacity to seamlessly integrate with other devices and systems depends on two factors: compliance with applicable standards and an evaluation of interoperability with such devices and systems (Kumar & Lu, 2019).

The confluence of the Internet of Things and the cloud emphasises the need of security protocols and standards. Selecting and tailoring protocols and standards to meet unique needs and risks is at the heart of every good security plan. Maintaining a safe Internet of Things (IoT) and cloud environment requires constant upkeep in the form of upgrades and adherence to best practises.

5. Cryptographic Techniques

When it comes to protecting data in the age of the Internet of Things (IoT) and cloud computing, cryptographic methods are at the very core of safety measures. These methods protect data against unauthorised access, modification, or deletion whether in motion or at rest. Within the context of Internet of Things (IoT) and cloud security, this section examines core cryptographic methods, such as encryption and decryption, Public Key Infrastructure (PKI), and safe key management.

5.1 Encryption and Decryption in IoT and Cloud

A mathematical method and a cryptographic key are used in the process of encryption, which transforms plaintext data into ciphertext. It makes information unintelligible to prying eyes. Using the correct decryption key, ciphertext may be transformed back into plaintext, completing the encryption process. Encryption is used to protect information while it is in transit and while it is stored in the cloud. Communication between IoT devices and cloud servers is often encrypted using protocols like TLS/SSL and IPsec while in transit. File- and disk-level encryption algorithms guarantee the security of data while it is resting in storage.

5.2 Public-Key Infrastructure (PKI)

The Public Key Infrastructure (PKI) is a system for controlling access to and usage of cryptographic keys and certificates. A CA, which is responsible for issuing digital certificates, a RA, which is responsible for verifying certificates, and a directory, which stores certificates, make up this infrastructure. Digital certificates are used for authentication between IoT devices and cloud services. To guarantee the reliability of connected devices and cloud infrastructure, PKI is an essential component of IoT and cloud security. It's a useful tool for warding against man-in-the-middle and other forms of network intrusion. Adams, Cain, Pinkas, and Zuccherato include X.509 for certificate formats and RSA and ECC algorithms for key generation as two of the most widely used Public Key Infrastructure (PKI) standards.

5.3 Secure Key Management

Cryptographic keys used for Internet of Things (IoT) and cloud security must be protected, hence secure key management is

crucial. In order to avoid key compromise, it is important to produce, store, and disseminate keys securely. Protecting cryptographic keys from both physical and logical threats requires the deployment of hardware security modules (HSMs). Datagram Transport Layer Security (DTLS) and similar lightweight key management protocols are used for efficient key exchange in the Internet of Things (IoT), where resource-constrained devices predominate. Regular key changes, strong encryption, and restricted access are all hallmarks of secure key management.

When it comes to protecting information and communications in the age of the Internet of Things and the cloud, cryptographic methods are essential. A complete security plan must include strong encryption, PKI, and secure key management practises. Maintaining a safe IoT and cloud environment relies heavily on these methods of protecting data's privacy, integrity, and authenticity.

6. Identity and Access Management (IAM)

Convergence of IoT and cloud computing makes Identity and Access Management (IAM) an essential part of security. IAM systems are crucial to the security of data and systems because they restrict access to those who are authorised to use them. The significance of Identity and Access Management (IAM) in the context of Internet of Things (IoT) and cloud security is discussed in this section.

6.1 Role-Based Access Control (RBAC)

A security paradigm known as role-based access control (RBAC) allocates privileges to various parts of an organisation rather than to specific users. RBAC is used to manage and regulate access to devices, services, and data in IoT and cloud settings. By allowing administrators to assign roles to individuals or devices, RBAC streamlines the access management process. A "sensor" job on an IoT device, for instance, could simply be able to read data, whereas an "administrator" role would have complete authority over the device. The danger of unauthorised access or data breaches is reduced by using this paradigm since access is restricted to just what is required for each position.

6.2 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security method that calls for more than one form of authentication from a person or device before allowing access. Things you know (passwords), things you have (tokens, smart cards), and things you are (biometric data) are all common components in authentication. Multi-factor authentication (MFA) strengthens access control in IoT and cloud environments. For instance, users may need to give a password in addition to a fingerprint scan or a one-time code issued by a mobile app when accessing IoT devices or cloud services. The danger of unauthorised access is greatly reduced with multi-factor authentication (MFA) (Rahman, 2016), even if one of the factors is compromised.

6.3 Federated Identity Management

A user's identity and authentication may be used across various domains or organisations thanks to federated identity management. Federated identity management allows for easy and safe access to resources hosted by many service providers

in IoT and cloud ecosystems. A user with a federated identity, for instance, may log in to numerous Internet of Things (IoT) gadgets, cloud apps, and service providers with only one set of credentials. This streamlines user administration and improves the overall service. Secure identity federation across IoT and cloud settings is made possible by federated identity management protocols like Security Assertion Markup Language (SAML) and OpenID Connect. Integrating IAM is crucial for protecting cloud and IoT infrastructures. An efficient IAM approach will include RBAC, MFA, and federated identity management. They guarantee the safety and integrity of IoT and cloud ecosystems by providing fine-grained control over access, improving authentication procedures, and streamlining user administration.

7. Threat Detection and Intrusion Prevention

Security measures for the Internet of Things (IoT) and cloud computing must include both threat detection and intrusion prevention. Within the context of Internet of Things (IoT) and cloud security, this section examines critical facets of threat detection, such as Intrusion Detection Systems (IDS), anomaly detection approaches, and real-time threat monitoring.

7.1 Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are a kind of security device used to keep systems safe by keeping tabs on all the activity happening on them or passing through them. Two broad types of IDS have been identified:

Network-based IDS (NIDS): Security systems that monitor networks for malicious activity are called network intrusion detection systems (NIDS). NIDS may detect anomalous communication patterns between devices or attempts to exploit vulnerabilities in IoT and cloud systems.

Host-based IDS (HIDS): Host intrusion detection systems (HIDS) are used to keep tabs on what's happening on local computers and servers. To identify malicious activity or suspicious patterns, it examines system logs, file modifications, and running programmes. HIDS in cloud settings may detect anomalous system activity and unauthorised access to cloud instances.

The ability to quickly identify and react to threats is essential for the protection of IoT devices and cloud services, and this is where intrusion detection systems (IDS) shine.

7.2 Anomaly Detection Techniques

Anomaly detection methods seek for and catalogue irregularities in normally occurring data. These methods are crucial in the fight against cybercrime and the protection of sensitive data stored in the cloud and on the Internet of Things. Methods often used for detecting anomalies include:

Statistical Analysis: Statistical modelling relies on the examination of past events to predict future patterns of behaviour. Anomalies are detected as departures from this norm. This method may identify out-of-the-ordinary activity or traffic patterns in the IoT.

Machine Learning: Algorithms trained on huge datasets may be used to spot outliers. These algorithms are able to detect even the most minute changes in network activity, user habits, or system operations.

Behavioral Analysis: Analysis of user and device behaviour in relation to a system is known as "behavioural analysis." It is able to detect suspicious actions by examining those that are out of the ordinary (He & Wu, 2019).

7.3 Real-Time Threat Monitoring

In order to detect and react to threats as they occur in real time, real-time threat monitoring requires constant monitoring of network traffic, system activity, and user behaviour. Tools for real-time monitoring offer:

Alerting and Notification: Security personnel are able to react swiftly to threats thanks to warnings and notifications generated by real-time monitoring systems whenever suspicious activity or abnormalities are discovered.

Logging and Forensics: Real-time monitoring technologies record data for analysis and forensics after the fact. According to Whitman and Mattord, this aids security teams in their investigation of events and identification of attack pathways.

Automated Responses: Isolating hacked IoT devices or blocking malicious traffic are two examples of the kinds of automatic actions that may be triggered by certain real-time monitoring systems (Schneier, 2000).

The security posture of IoT and cloud settings depends heavily on threat detection and intrusion prevention. Effective identification and mitigation of security risks are aided by intrusion detection systems, anomaly detection methods, and real-time threat monitoring. The overall security of IoT and cloud ecosystems may be improved by combining these technologies and practises.

8. Security in Cloud Environments

Because information and programmes are stored and run on other servers, cloud computing places an emphasis on security. Protecting sensitive data and keeping users' confidence necessitates implementing stringent security protocols. Security-as-a-Service (SECaaS), cloud-native security solutions, and the shared responsibility paradigm are all discussed in this section since they are fundamental to cloud security.

8.1 Security-as-a-Service (SECaaS)

Subscription-based Security-as-a-Service (SECaaS) is a cloud-based service model that provides security solutions. In the cloud, it has a number of benefits:

Scalability: SECaaS solutions are scalable, meaning they can be expanded or contracted as needed. The ability to adjust to new circumstances is essential for effective security.

Cost-Efficiency: Organisations may save money by not having to buy and maintain expensive security gear and software on

their own facilities. Instead of investing in expensive hardware, businesses may save money by subscribing to SECaaS.

Expertise: SECaaS suppliers usually employ cybersecurity professionals that update and maintain security measures on a consistent basis, demonstrating their proficiency in this area. As a result, businesses may take use of employees' unique sets of skills and expertise.

8.2 Cloud-Native Security Solutions

Cloud-native security solutions are built from the ground up to protect cloud infrastructures and applications. The following are important tenets of cloud-native security:

Microservices and Containers: To further improve application security, cloud-native security makes use of microservices and containerization. Due to its compartmentalization, containers limit the spread of a security compromise laterally (Burns et al., 2016).

Serverless Computing: The security burden of serverless computing is transferred to the cloud service provider, lowering the attack surface for businesses. Nonetheless, businesses must ensure the safety of their software and customer information (Roberts et al., 2018).

API Security: Cloud-native apps rely heavily on Application Programming Interfaces (APIs), making API security a top priority. Protecting data and services requires properly securing APIs, which includes using strong authentication and permissions (OASIS, 2019).

8.3 Shared Responsibility Model

The principle of shared accountability is fundamental to cloud security. It specifies how cloud providers and clients should divide up security duties. Each form of cloud service has its own unique structure:

Infrastructure as a Service (IaaS): With IaaS, the cloud provider takes care of protecting the underlying system (such as servers, networks, and virtualization), but the user is responsible for securing the software they're using and the information it stores (AWS, 2021).

Platform as a Service (PaaS): With PaaS, the cloud service provider takes care of protecting the underlying system, while the user is responsible for the safety of their own data and applications.

Software as a Service (SaaS): While the consumer is responsible for data security and access control in SaaS, the cloud provider is in charge of safeguarding the whole stack (infrastructure, platform, and apps) (Microsoft, 2021).

Providing safety in a cloud setting is complex. Cloud-native security makes use of cloud technology to provide better protection, while security-as-a-service (SECaaS) provides adaptable and inexpensive solutions. In order to handle cloud security efficiently, businesses must have a firm grasp of the shared responsibility paradigm.

9. Conclusion:

The confluence of IoT and cloud computing provides a complex and ever-evolving environment of security issues, but also offers enormous opportunity for creativity and efficiency. Many of these difficulties, as well as possible solutions, have been investigated in depth in this extensive study. We looked at the impact of IoT and cloud computing in the modern digital environment, appreciating their potential to revolutionise many different sectors. We did, however, recognise that a number of security difficulties, such as data privacy, authentication and authorization problems, data integrity, scalability limitations in IoT devices, and the ever-present danger of insider assaults and external breaches, arise as a result of this convergence. The research outlined important strategies and solutions for overcoming these obstacles. Methods like identity and access management tactics for limiting user rights and sophisticated threat detection and intrusion prevention systems are examples of these stringent security procedures and standards. Security-as-a-Service (SECaaS) and cloud-native security solutions were

also highlighted as being crucial to adjusting to the ever-changing nature of the threat environment.

The survey also highlighted the shared responsibility approach, which establishes a division of labour in terms of security between cloud service providers and their clients. Organisations must be proactive and diligent in tackling these security risks as they navigate the confluence of IoT and cloud computing. If the benefits of the Internet of Things (IoT) and cloud computing are to be fully realised without jeopardising the security, privacy, and reliability of stored information and services, then ongoing research, innovation, and stakeholder engagement are required. The pursuit of effective security measures will continue to be important as technology develops and as the Internet of Things (IoT) and cloud computing become more pervasive in our everyday lives and in many businesses. Organisations may strengthen their IoT and cloud defences against new threats by following the guidelines and suggestions presented in this study, creating a more secure and robust digital ecosystem in the long run.

References

- [1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.
- [2] AWS. (2021). Shared Responsibility Model. Amazon Web Services. Retrieved from <https://aws.amazon.com/compliance/shared-responsibility-model/>
- [3] Banijamali, A., Pakanen, O. P., Kuvaja, P., & Oivo, M. (2020). Software architectures of the convergence of cloud computing and the Internet of Things: A systematic literature review. *Information and Software Technology*, 122, 106271.
- [4] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, 56, 684-700.
- [5] Burns, B., Grant, B., Oppenheimer, D., Brewer, E. A., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. *ACM Transactions on Computer Systems*, 34(3), 1-24.
- [6] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST Standard for Role-Based Access Control. *ACM Transactions on Information and System Security*, 4(3), 224-274.
- [7] Ghose, A., Acquisti, A., & Telang, R. (2016). Does Privacy Protection Make Agents Angry? The Impact of Privacy Protection on Economic Transactions in E-Markets. *Information Systems Research*, 27(2), 440-456.
- [8] Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, 5, 41-70.
- [9] He, X., & Wu, X. (2019). A Survey of Anomaly Detection in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, 15(10), 5655-5663.
- [10] Khan, R., Salah, K., & Almaini, A. E. (2018). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *IEEE Access*, 6, 8587-8603.
- [11] Kumar, S., & Lu, R. (2019). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. *Journal of Ambient Intelligence and Humanized Computing*, 10(9), 3535-3562.
- [12] Mamun-Ibn-Abdullah, M., Shahinuzzaman, M., Rahim, S. A., & Kabir, M. H. (2020). Convergence platform of cloud computing and Internet of Things (IoT) for smart healthcare application. *Journal of Computer and Communications*, 8(8), 1-11.
- [13] Microsoft. (2021). Shared Responsibility Security Model. Microsoft Azure. Retrieved from <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
- [14] OASIS. (2019). OWASP Application Security Verification Standard 4.0. OASIS Standard. Retrieved from https://www.oasis-open.org/committees/document.php?document_id=65306

- [15] Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016, March). Securing sensor to cloud ecosystem using internet of things (iot) security framework. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (pp. 1-5).
- [16] Rahman, S. A. (2016). Multi-Factor Authentication. In *Security and Privacy in Communication Networks* (pp. 207-218). Springer.
- [17] Ray, P. P., Dash, D., & De, D. (2018). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 253-279). IGI Global.
- [18] Raza, S., Shafagh, H., Hewage, K. A. S., Hummen, R., & Voigt, T. (2019). Lithe: Lightweight Secure CoAP for the Internet of Things. *IEEE Sensors Journal*, 19(9), 3260-3268.
- [19] Roberts, J., Islam, S., Yan, K., & Zeldovich, N. (2018). Valet: A Language for Proof-Carrying Code with Rich Certificates. *Proceedings of the 39th ACM SIGPLAN Conference on Programming Language Design and Implementation*.
- [20] Sharma, P. K., Singh, S., & Park, J. H. (2018). OpCloudSec: Open cloud software defined wireless network security for the Internet of Things. *Computer Communications*, 122, 1-8.
- [21] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2015). Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks*, 76, 146-164.
- [22] Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In *2015 International conference on green computing and internet of things (ICGCIoT)* (pp. 1577-1581). Ieee.
- [23] Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., ... & Fratu, O. (2015). Big data, internet of things and cloud convergence—an architecture for secure e-health applications. *Journal of medical systems*, 39, 1-8.
- [24] Yu, S., Tian, H., & Guizani, M. (2019). Internet of Things (IoT) Security: Current Status, Challenges and Prospective Solutions. *IEEE Internet of Things Journal*, 7(12), 12636-12649.