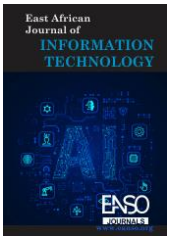


East African Journal of Information Technology
eajit.eanso.org
Volume 6, Issue 1, 2023
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review

Elton Luvaha[1*], *Lamek Ronoh*[1] *& James Abila*[1]

[1] Rongo University, P. O. Box 103 – 40404, Rongo, Kenya.
* Correspondance ORCID ID: https://orcid.org/0009-0003-1464-3955; Email: eltonomukuba@gmail.com

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

Date Published: *27 July 2023*

Keywords:
Data Privacy, Privacy Technologies, Attack Surfaces, Privacy Dangers.

ABSTRACT

With the rollout of the Fifth-Generation network, more Internet of Things (IoT) devices tend to increase, which increases the amount of data being shared by the devices. It is complex to secure data transmission and device-to-device communication due to the vast number of IoT devices and the complexity of networks. The Internet of Things (IoT) has evolved to enable everyday things and gadgets to connect digitally and communicate with one another, using technologies that send, gather, and analyse data from people using those objects and devices. IoT data privacy risks are widespread use. The primary objective of information technology (IT) security in Web 2.0 was to ensure the privacy, accuracy, and reliability of systems and communications. As a result of IoT devices' often limited CPU power for longer-lasting activities, these conventional metrics, however, exhibit measurable constraints. IoT security is, therefore, critical in the context of guaranteeing security through the data privacy of IoT users. The author conducted a literature methodological analysis on the data privacy framework that will help to safeguard the 5G IoT-enabled devices on user data, technologies for data privacy in 5 G-based IoT devices, data privacy dangers associated with 5G IoT devices, and data privacy attack surfaces in 5G IoT devices.

APA CITATION
Luvaha, E., Ronoh, L. & Abila, J. (2023). Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review. *East African Journal of Information Technology*, *6*(1), 119-134. https://doi.org/10.37284/eajit.6.1.1333

CHICAGO CITATION
Luvaha, Elton, Lamek Ronoh and James Abila. 2023. "Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review". *East African Journal of Information Technology* 6 (1), 119-134. https://doi.org/10.37284/eajit.6.1.1333.

HARVARD CITATION
Luvaha, E., Ronoh, L. & Abila, J. (2023) "Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review", *East African Journal of Information Technology*, 6(1), pp. 119-134. doi: 10.37284/eajit.6.1.1333.

IEEE CITATION
E. Luvaha, L. Ronoh & J. Abila, "Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review", *EAJIT*, vol. 6, no. 1, pp. 119-134, Jul. 2023.

MLA CITATION
Luvaha, Elton, Lamek Ronoh & James Abila. "Data Privacy, Conceptual Framework for IoT Based Devices in Healthcare: A Systematic Review". *East African Journal of Education Studies*, Vol. 6, no. 1, Jul. 2023, pp. 119-134, doi:10.37284/eajit.6.1.1333.

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

INTRODUCTION

The Internet of Things (IoT) and fifth-generation cellular (5G) technology are among the trending technologies that have shown significant applications in virtually all task domains of human endeavours. Some of the emerging application areas are; augmented reality, high-definition video streaming, self-driving cars, smart environments, e-health care, etc. These applications are characterised by higher data rates, wider bandwidth, more data sharing capacity, low latency, and high throughput.

Despite all the positive aspects, Data transmission, data security, and data collecting are the three key issues with IoT, 5 G-based devices. According to (Azrour, Mabrouki, Guezzaz, & Kanwal, 2021), data security is not given the attention it deserves. A flaw in the authentication of such devices can result in a variety of assaults, such as the replay attack, the Denning-Sacco attack, a denial-of-service attack, a password guessing attack, etc.

As the number of IoT devices grows, so does the requirement for a fast internet connection and a secure environment through 5G network technology (Ahmad et al., 2018). IoT has led to an increase in data availability making it easier to collect personal data; therefore, there is exponentially growing and unavoidably endanger in the confidentiality and integrity of data (Nyemba, 2019).

According to (Feng, Deng, & Chen, 2019), IoT device owners are exposed to serious vulnerabilities due to security and privacy leakage issues from IoT devices. Data volume and complexity increase as more gadgets connect to the Internet or other networks, which increases the risk of becoming vulnerable. This necessitates that the users' or individuals' integrity and confidentiality must be preserved when the data acquired by these devices is stored securely on a large scale. According to a report by (Palo Alto Networks, 2020), personal and confidential information is exposed since 98% of all IoT traffic is not encrypted.

IoT devices should be equipped with authentication, authorisation procedures, and data preservation capabilities to combat illegal access, data theft, and eavesdropping (Catania & La Corte, 2018). This will guarantee that information is current, authentic, confidential, and intact.

This study reviews the literature on data privacy and establishes a systematic literature on a conceptual framework that is suitable for maintaining data privacy in IoT-based medical devices. In order to safeguard user privacy and maintain the confidentiality and integrity of acquired data, it underscores the significance of resolving data security issues and the necessity of systems for authentication, authorisation, and data storage. The paper is an important source of knowledge in the current sophisticated cyber landscape where there is a shifted malicious target and distributed blockchain attacks targeting healthcare data with great sensitivity to personal identity.

LITERATURE REVIEW

Privacy Dangers Associated with 5G IoT-Based Devices

Data Privacy dangers come in varying forms during the Collection, use, and disclosure of private data, Transparency, De-identification of data, Authentication, and Integrity. The details of the dangers are discussed in the next section, which includes.

Collection, Use, and Disclosure of Private Data

When collecting data from those who have no option but to provide it, particular attention is not usually paid to the purposes for which it will be utilised. For instance, utility companies may decide to stop selling and providing assistance for conventional energy meters due to energy efficiency and ease of maintenance brought about by smart meters (Balough, 2011), which will force the residents to use the smart meters. Smart energy meters can expose a variety of highly private details about people (Rajagopalan, Sankar, Mohajer, & Poor, 2011). Both overt details like how frequently they use their washing machine,

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

and covert details, like what television shows they watch, can be collected by smart meters. Data and interpretations from IoT devices like smart meters are anticipated to be immensely valuable to organisations like insurers, advertisers, employers, and law enforcement (National Institute of Standards and Technology, 2010).

Transparency

It can be challenging for people to be notified that their personal information is being collected due to the passive nature of many IoT devices. Devices in public places can automatically collect information, yet occasionally they rely on people to choose not to if they do not want it to. Opt-out models, however, have trouble operating because many IoT devices lack interactive features. Users may be unaware that their data is being gathered, let alone that they have the option to refuse such acquisition. For instance, In the Matter of Nomi Technologies, Inc. (United States of America before the Federal Trade Commission, Docket No. C-4538, August 28 2015), Nomi was accused of acquiring and using consumer information without their consent. It was further accused that through its "Listen" service, Nomi leverages mobile device tracking technologies to offer analytics services to brick-and-mortar stores. Since January 2013, Nomi has been gathering data from users' mobile devices to deliver the Listen service (Tushnet, 2009).

It can be challenging to locate relevant data when people wish to enlighten themselves on how personal information a gadget gathers and how that data is utilised. IoT devices generally lack input devices like keyboards and displays like screens, making it challenging for them to convey illuminating information like privacy policies (Office of the Victorian Information Commissioner, 2021).

According to the Office of the Australian Information Commissioner (Office of the Australian Information Commissioner, 2016), a report by the Australian Privacy Commission and fellow international regulators through the Global Privacy Enforcement Network, privacy policies of over 300 businesses around the world, including 45 by Australian consumers, and the following results were found;

- 71% were unable to adequately describe how information was stored.
- 69% did not adequately explain how customers could delete their information from the device
- 38% omitted accessible contact information if customers expressed privacy concerns.
- 91% of businesses did not inform that users can modify their privacy preferences.

Organisations are attempting to exploit intellectual property rights to protect the way an IoT device gathers or uses personal information; the data acquired by devices or the inferences and insights gained from that data may make it more difficult to ensure the transparency of IoT devices (Australian Government, 2017).

Lack of De-Identification of Data

Large IoT ecosystems, like smart cities, generate a lot of data that might be used for a variety of things, including legislative decision-making and research. Making this data accessible to the public online is a frequent strategy to maximise its usefulness. Sensitive personal information, nonetheless, should never be shared with the public. Allowing people to stay anonymous by not even gathering information that can identify them is the easiest way of ensuring that personal information is not included in a dataset. De-identification is the technique of deleting private information from a dataset. Unfortunately, due to the highly detailed nature of the IoT data generated, it is frequently exceedingly challenging to de-identify data (Peppet, 2014).

Organisations frequently use hashing, which tries to modify the data using an algorithm, to try to eliminate sensitive information from data acquired from IoT devices (GSMA, 2019). Hashing replaces an identifiable person with what is essentially a unique identification, pseudonymising information instead of

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

permanently de-identifying it. Although hashing can sometimes be effective for shielding personal information, it is typically quite simple to re-identify information that has been hashed. For instance, a New York resident-proclaimed civic hacker was able to use information from Taxi and Limousine Commission (TLC) to re-identify information about taxi drivers by rewriting new hash functions (Ducklin, 2014).

If indeed the dataset is being used in training an AI model that is then released, information about the persons in the dataset may be disclosed. AI could extrapolate personal or even confidential information from the dataset, which becomes a risk when sharing de-identified data (Ateniese et al., 2015).

Lack of Authentication

Due to the large number of devices, the greatest issue in the IoT network is thought to be the authentication service. It incorporates identity verification. The devices must be able to verify the authenticity and validity of remote users on a public network during the authentication process. Earlier authentication methods relied just on a single factor, which was a straightforward password. These approaches must deal with several password-related problems, though. Users can quickly forget their password to start. Additionally, people might use weak passwords. Finally, either by a dictionary attack or an extensive research effort, the attackers are successful in guessing the right password (Azrour et al., 2021). Password-based authentication therefore cannot guarantee security on its own.

There are difficulties when people try to access the personal data that IoT devices have acquired about them. It is not a guarantee that an IoT device will have a single user or that the user will be the device's owner (Sarma & Girão, 2009). This implies that an IoT device may enable users to access the personal information of other people as well as gather and retain information on a variety of people (Geeng & Roesner, 2019). The lack of interfaces can make it difficult for devices to authenticate users and ensure they can only access information about themselves, which makes this a challenging problem to handle in terms of data security.

To reliably exchange data and keys between two entities, a legitimate connection between them must be established. Mutual authentication is necessary for the IoT environment because IoT data are employed in various decision-making and actuation processes. To counteract impersonation, stringent authentication procedures must be implemented. There are tight restrictions on the use of any authentication approach due to the resource limitations of IoT devices (Tiburski, Amaral, & Hessel, 2016). This poses a security challenge for users' data who use IoT devices.

Lack of Data Integrity

According to Lundgren and Möller(Lundgren & Möller, 2019), integrity refers to the fact that no unauthorised party altered the message during transmission. As a result, it ensures that the recipient has gotten the full message from the source. The basic goal is to prevent an unauthorised person from illegally modifying information. The system needs to ensure data integrity to maintain the security of smart devices in IoT networks. IoT organisations share crucial data with other establishments and place a strict requirement that data collected, stored, and sent not be altered mistakenly or maliciously. Message authentication codes (MAC) that employ one-way hash functions can be used to guarantee data Integrity (Van & Thuc, 2015). The choice of the MAC approach depends on the capability of the device.

Accelerators of Data Privacy Dangers in IoT Devices.

5G networks are ready to meet the predicted increase in IoT devices and related technologies. With the arrival of 5G networks comes an increased demand for security and privacy.

The first step in studying cellular wireless security is determining the security goals. The security policy and associated technology, in this case, IoT devices, should guarantee that information

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

created by or linked to a user is appropriately safeguarded against abuse or theft. It must be assured that the degree of protection supplied to consumers and suppliers of services is deemed to be superior to that provided in modern wired and wireless networks. Furthermore, it can be observed that the deployment of security features and methods may be enhanced and improved when new threats and services emerge (Magalakshmi & Kumar, 2017).

In today's technologically advanced world, every gadget that a person uses is linked to the Internet. This raises the likelihood of private information being leaked. This is the main disadvantage of such communication. If information is not managed appropriately, sensitive information may be disclosed to a third party (Wazid, Das, Shetty, Gope, & Rodrigues, 2020).

Firmware Vulnerability

The Multi-Access Edge Compute (MEC) within the 5G architecture creates an attack surface. Unlike traditional network deployments, MEC provides fundamental traffic capabilities such as data processing and storage within telecommunication networks. The existence of system components in the MEC, including hypervisors, operating systems, and apps, may enable malicious actors with additional attack vectors to intercept, manipulate, and destroy sensitive data. Untrusted components or malware implanted inside the MEC may compromise user privacy by allowing hostile actors to clone devices and impersonate end-users to make calls, send messages, and access data. Untrusted components or malware can be used by malicious actors to obtain access to the MEC and end-user components, allowing them to get access to the larger radio access network (National Security Agency, 2021).

With the firmware vulnerability, a malicious actor can take advantage of this and gain access and later compromise the network's confidentiality, integrity, and availability by stealing sensitive sensor and user equipment data, changing data streams, and blocking access to certain data or sensor streams. The malicious actor now has enough bandwidth to acquire complete access to the RAN and clone end-user devices such as the IoT devices, which contain sensitive user information.

Lack of Standardisation.

IoT devices create massive amounts of data, which necessitates effective security. However, owing to a lack of standardisation with a wide range of hardware and software, the deployed devices are subject to different threats and assaults (Anwar, Zainal, Abdullah, & Iqbal, 2020). If IoT devices are used in sensitive areas, such as healthcare, where these devices convey patient-related information to or between other networks and devices, data security and privacy are vital. Similarly, IoT devices that store personal, consumer, or commercial data must be safeguarded and secure against theft and manipulation. In terms of security, many IoT devices are built with weak or non-existent cyber-security safeguards. Hackers are using these gadgets as access points into company networks.

Edge Layer Attacks Accelerators

IoT gadgets have linked millions of homes worldwide over the Internet. Threats from hardware Trojans (HT) in integrated circuits (IC) have recently become a major worry, affecting IoT edge devices (IoT-ED) (Mohammed, Hasan, & Awwad, 2020). IoT device manufacturers have produced different devices, with each having its hardware standards more so in terms of security. IoT devices are exposed to edge layer attacks which consist of the hardware components where the operating system is embedded. Side channel attacks are one of the most serious risks at this level (A. Singh, Chawla, Ko, Kar, & Mukhopadhyay, 2019). The purpose of these attacks is to leak information by analysing side signals like power usage, electromagnetic emissions, and communication time while nodes are encrypting. Among these, the gadgets' power consumption is commonly used to anticipate and acquire encryption secret keys (Meneghello, Calore, Zucchetto, Polese, & Zanella, 2019).

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

Most IoT devices can be put in remote locations with a minimal level of security, allowing an unauthorised user to launch side-channel attacks due to the vulnerabilities in the edge layer. If the hacker succeeds, people's personal information will be in danger.

Application Layer.

This layer guarantees data integrity, secrecy, and authenticity. The protocols at the application layer establish the application interface with the lower layer protocols for data transmission over the network. Using ports, application layer protocols enable process-to-process connectivity. The application layer protocols include; Web socket, HTTP, CoAP, DDS, MQTT, AMQP, and XMPP.

There are various security issues in this layer which include; Identity verification, where various users will choose different apps, and each application will have a large number of users; thus, a robust authentication method should be established to prevent unauthorised users from gaining access to the system. Storage of data and recovery is also a security issue for the user's data. Data storage entails data transit across many routes to various places, which concerns user privacy and data integrity. And the subsequent recovery of such data on time. Many security concerns exist during data transfer. As a result, effective data storage and recovery should be implemented at every stage of data transfer (Meneghello et al., 2019).

Vulnerabilities in application layer software also raise a great concern for the privacy of data in IoT devices. Buffer overflow vulnerabilities can emerge when software developers write non-standard code. Hackers may utilise these exploits to further their goals.

Lack of Access and Authentication between Device

The globe is presently seeing the transformation of wireless mobile communication technology into its fifth generation. Device-to-device (D2D) communication is one of the key aspects of the 3rd Generation Partnership Project's Release 12. (3GPP) (Kar & Sanyal, 2020). The 3GPP mobile broadband standard community established D2D to set the groundwork for developing 5G architecture and enabling off-grid connectivity.

To enable communication between devices, conventional cellular mobile communication technology employs a network infrastructure architecture comprised of base stations (BSs) and a core network (CN). Even though the sources and destinations are near to one another, data is always routed through the cellular network architecture. D2D allows numerous devices to interact without passing through intermediary access points (APs) and base stations (BSs), decreasing CN reliance.

With the growing need for IoT and other communication devices, different manufacturers and developers implement different systems which compromise security which in turn might lead to system performance issues. D2D communication creates a link between the devices. As a result, the devices are vulnerable to a variety of security risks, including data falsification, user privacy invasion, and alteration (Panicker, Salehi, & Rudolph, 2021). Due to the exposed nature of the wireless connection, information transmission between D2D users is more susceptible.

A serious threat to D2D devices may be seen in an attack on privacy. Rogue devices attempt to access a device's data. The location and user information are among these device attributes. Once obtained, these parameters can occasionally be quite important since they expose the details about the subject that the malicious device needs to know. It is risky to communicate sensitive data to UE devices you have never encountered before. Additionally, it may pave the way for fresh issues like eavesdropping and location spoofing (Haus, Waqas, Ding, Li, & Member, 2017).

IoT Application in Health and Emerging Data Issues

The uses and most recent developments of IoT in the healthcare industry are covered in this section. By utilising IoT in healthcare, new opportunities have been opened for providing top-notch

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

healthcare services to people everywhere, making it simpler for people to get in touch with and use healthcare services whenever they need them.

With all the benefits IoT comes within the health sector, there are also challenges in addressing the security and privacy of data. IoT-based healthcare applications and devices are anticipated to deal with sensitive individual data, such as private health information. These intelligent gadgets may be connected to a global information network to make it simple to access them at any time from any location (Rghioi, L'aarje, Elouaai, & Bouhorma, 2014).

According to a recent study by healthcare cybersecurity provider Cynerio, 56% of hospitals have had their IoT/IoMT devices attacked in the past two years. 88% of data breaches involved IoT devices. An alarming figure is that 53% of medical IoT devices have at least one critical vulnerability (Colquhoun, 2022).

A study conducted by (Krishnan, 2023) had the following findings;

- In the last two years, 56% of firms suffered at least one hack using an IoT or IoMT device, and 24% of them reported adverse impacts leading to higher mortality rates.
- Since 2020, 65% of the respondents have experienced an average of five or more data breaches, with 88% of those incidents involving IoT and IoMT devices.
- Only 21% of respondents reported having proactive security measures in place, even though 71% of respondents ranked the risk presented by IoMT devices as high or very high.

It is vital to quickly recognise and assess various IoT security and privacy challenges, including current and anticipated security issues, security requirements, vulnerabilities, threat models, and various approaches to provide more robust security, as the use of IoT in healthcare is beset by many security challenges that, if not properly managed, could impede the full adoption and application of IoT in the health sector.

According to a report by Cynerio (Cynerio, 2022), 38% of a hospital's IoT equipment consists of infusion pumps, also known as IV pumps. According to the same report, 73% of IV pumps have flaws that hackers might use to jeopardise patients' security and data privacy. Additionally, access points that limit access to rooms and VoIP devices that allow for doctor-to-lab-technician contact pose additional security threats. These might be compromised or rendered useless by attackers during a ransomware attack if left unattended, which would have disastrous effects on patient outcomes.

The security and privacy issues are not limited to;

Impersonation.

IoT-based network gadgets are no exception, as each one has a unique identity and may hold patient data. If a hacker were to obtain this identity, he might use it to spy on the patient's medical records.

Data modification.

It could be disastrous for patients whose health is being tracked by the use of IoT devices if a malicious party intercepts medical data sent by a patient, either from the source node of an IoT-based device or during data exchange between nodes. By altering the data, the malicious party could present the wrong information to caregivers, who would then react accordingly.

Eavesdropping.

IoT devices employ wireless channels to communicate, which makes it simpler for an outsider to be able to listen in on the conversations between nodes, jeopardising the security of the patient's data and allowing for more harmful assaults to be carried out using such data.

Sensor tracking.

Many MTs use GPS sensors in geriatric health monitoring systems to relay the patient's location during an emergency. Attackers may use insecure gadgets to spoof GPS data or learn the locations of patients (Jafarnia-Jahromi, Broumandan, Nielsen, & Lachapelle, 2012). Similar

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

vulnerabilities can be found in various sensors used in systems such as wheelchair management, fall detection, and remote monitoring systems, exposing sensitive patient data. Similarly to this, MTs could be compromised by flaws in cellular networks' Signalling System No. 7 (SS7) (Gibbs, 2016).

According to (Cynerio, 2022), with all the benefits comes the possibility of new security threats and weaknesses in healthcare systems, which is why IoT application is also accompanied by these risks due to the following reasons;

- The majority of sensitive patient data is collected and shared by medical devices.
- Complexity and compatibility problems are brought on by the nature of IoT technology.
- Security features are not a priority for manufacturers of medical IoT devices.

Confidentiality, integrity, and availability (CIA) security concerns are growing as a result of the aforementioned factors mentioned above. This therefore calls for improved security and privacy mechanisms, which will enhance the privacy and security of data.

Security and Privacy Enhancing Technologies for Securing 5G IoT-Based Devices.

Blockchain-Based Security

The use of blockchain technology in this 5G-IoT situation, which typically involves a trusted intermediary, obviously improves the resilience and authenticity of the data involved. A block essentially comprises transaction data, a timestamp, a cryptographic hash function, a reference to the preceding block, and, if necessary, smart contracts (Sicari, Rizzardi, & Coen-Porisini, 2020). Qian et al. (Qian et al., 2018) suggested a unique, sophisticated security management technique using algorithms for different levels of IoT architecture based on blockchain. To assure security and reliability, a device identification-based key algorithm was developed based on the interaction between IoT devices and blockchain databases.

Centralisation is a security challenge in IoT devices as it creates peer-to-peer communication, which has drawbacks such as DDoS attacks, Listening Queries, Leechers, and content verification (Johnson, Mcguire, & Willey, 2016). Blockchain is a distributed ledger, and the key feature of this technology is decentralisation, which eliminates the intermediary between transactions. The use of Blockchain in IoT helps to eliminate centralisation and make transactions more safe, autonomous and transparent. The universal ledger in this architecture is blockchain, and it stores all messages between smart devices as trustworthy (Haris & Al-Maadeed, 2020).

Maintaining data integrity by using checksums or digital signatures to ensure data has not been altered. As a decentralised distributed ledger for IoT data, blockchain provides a scalable and robust solution to ensure the integrity of IoT data (Aravindhan P & Shamir Adleman, 2008).

Blockchain technology comes along with its strengths which include;

Immutable Data Integrity

A blockchain system's distributed ledger is impenetrable to manipulation. Each transaction is documented, stored in a data block, and added to an unalterable, secure data chain. The massive amounts of data that IoT devices create are not under the authority of any one organisation.

A new block is made and added to the chain whenever the state needs to be updated with new data. The state is only altered by adding new blocks, except for temporary forks, which are resolved by wiping off the most recent blocks. A block is deemed immutable once a certain amount of time has passed since it is no longer practicable to edit or remove it (Landerreche & Stevens, 2018).

Data that has been recorded on the blockchain cannot be readily changed or tampered with because of the immutability of the blockchain. With the help of this attribute, it is possible to confirm the accuracy of IoT data and give confidence that it was not altered during storage

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

or transmission. Because it eliminates the requirement for trust between the parties involved, immutability is viewed as one of the key benefits of blockchain-based smart contracts.

Improved Security.

Blockchain's powerful data tampering security helps prevent a fraudulent device from interrupting communications network synergy by inserting or relaying bad information. Using blockchain to contain IoT data would therefore add an extra degree of protection that hackers would have to go beyond to gain network access. As a result, blockchain technology can safely unlock the economic and operational values of 5G networks to enable basic operations like detecting, processing, storing, and transferring data.

According to (Gong-Guo & Wan, 2021), IoT devices can use secure authentication methods made possible by blockchain. The authentication process is made stronger by putting device IDs and related cryptographic keys on the blockchain, making it more difficult for hostile actors to spoof or modify device identities.

Assured integrity.

Blockchain and blockchain-based smart contracts may also help to secure the accountability and integrity of IoT networks. Smart contracts are software codes that enforce regulatory standards and make them visible (Mohanta, Panda, & Jena, 2018). These contracts rely entirely dependent on the openness and consistency of all member nodes. IoT device security policies can be automatically enforced using smart contracts, which are self-executing contracts with established rules and circumstances. To improve security and privacy, they can implement policies regarding data exchange, consent management, and access control. Blockchain's far stronger degree of encryption makes it practically hard to erase existing data records.

Weaknesses of Blockchain

Despite the benefits, there are certain restrictions with blockchain technology. In IoT situations with a large number of devices producing significant data, blockchain networks may experience scalability and performance issues that could be problematic. Furthermore, the integration of blockchain with already-existing IoT systems can be labour- and resource-intensive.

In a blockchain, each transaction is validated by a digital signature, and blocks of transactions are connected by validating digital signatures. Due to the constraints of IoT computation infrastructure, transaction verification is a resource-intensive procedure. The scalability of cryptographic processes on Blockchain implementation will be limited in transaction verification and block creation (Hewa, Kalla, Nag, Ylianttila, & Liyanage, 2020).

Because of their resource-constrained technology, IoT devices offer greater attack surfaces and major limits in privacy enforcement. When considering blockchain, data privacy is not inbuilt because transactions are openly added to the ledger upon verification. There is no trust in IoT devices.

While Distributed Ledger Technology (DLT) designs promise to improve security, security remains a key concern in the design and deployment of shared infrastructures. Businesses must safeguard not just data, contracts, files, devices, and networks but also preserve privacy, verify identity, prevent theft/spoofing, as well as provide administration for autonomous device coordination and settlement. IoT simply extends these decisions all through the network architecture, whether in a large-scale production environment, a rural area with limited bandwidth for connectivity, or inside a smart home or retail context. DLT is not a solution for IoT security; rather, it raises additional design issues throughout the stack (Groopman, 2018).

Multifactor Authentication.

Multifactor Authentication (MFA) is a layered approach to physical and logical access security in which a system needs a user to submit a combination of two or more separate authenticators to validate a user's identity for

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

login. MFA improves security since unauthorised users are unable to complete the second authentication criterion and so cannot access the targeted physical area or computer system if one authenticator is compromised (Cybersecurity & Infrastructure Security Agency, 2022).

MFA aims to build a layered defence that makes it more difficult for an unauthorised individual to get access to a target, such as a physical place, computer equipment, network, or database. If one of the factors is hacked or broken, the attacker still has one or more hurdles to overcome before effectively entering the target (Shacklett, 2021). With the use of MFA, the privacy and security of user data can be assured through the techniques used for authentication should be lightweight for them to be supported by IoT devices.

AES Encryption Algorithms.

On September 12, 1997, the National Institute of Standards and Technology (NIST) released a formal request for algorithm submissions and announced the start of an initiative to create the AES. Daemen and Rijmen (Daemen & Rijmen, 2000) came up with the (AES) algorithm. Because of its higher security levels, it is anticipated to replace DES and Triple DES to satisfy the more stringent data security requirements (Nechvatal et al., 2001).

(AES) the technique is fast in both software and hardware and is based on the substitution-permutation network design idea, which combines substitution and permutation. It is based on the private-key cryptography algorithm, in which both encryption and decryption use the same keys. One can choose between 128, 192, or 256 bits for the data length of a key or message (Lu & Tseng, 2002). The long bit key makes the algorithm more secure since the longer the key, the harder it will be for the hackers to get into the system; thus can be considered an appropriate encryption technique to be applied.

Elliptic Curve Cryptography

A more recent form of public-key cryptography that outperforms Rivest–Shamir–Adleman (RSA) encryption is called elliptic curve cryptography. It is faster since shorter keys are used. Katiyar et al. (Katiyar, Dutta, & Gupta, 2010) asserted that elliptic curve cryptography is an active and effective public key cryptographic in the next generation of cryptosystems. Multiplication is an essential elliptic curve operation. In his discussion of earlier research on scalar multiplication algorithms, Karthikeyan examines critical factors such as hamming weight, efficiency, and memory needs.

Kumar et al. (Kumar, Chandra Sekhar, & Naidu, 2015) explored various elliptic curve applications in certain environments, such as phones, network sensors, PDAs, mobile networks, etc., and presented studies on elliptic curves in pervasive computing environments. Due to its adaptability for devices with low bandwidth, battery life, and memory requirements, elliptic curve cryptography became the dominant choice prior to exposure. Due to this elliptic curve, cryptography is suitable for IoT devices due to their limited processing power and memory.

IoT Attack Surfaces

Recognising the IoT's possible implications is also necessary, given its rising reality. For instance, IoT is frequently used in the office automation (OA) and operational technology (OT) sectors in an organisational context. Multiple IoT, IoMT, and IIoT devices can be deployed within an enterprise as a result. Such a setup increases the likelihood of threats in areas that previously offered no cybersecurity problems. IoT technology efforts will experience an immense expansion due to the potential to send more data more quickly due to the 5G network, which will increase their numbers, leading to more attack surfaces (G. P. Singh & Bangotra, 2021).

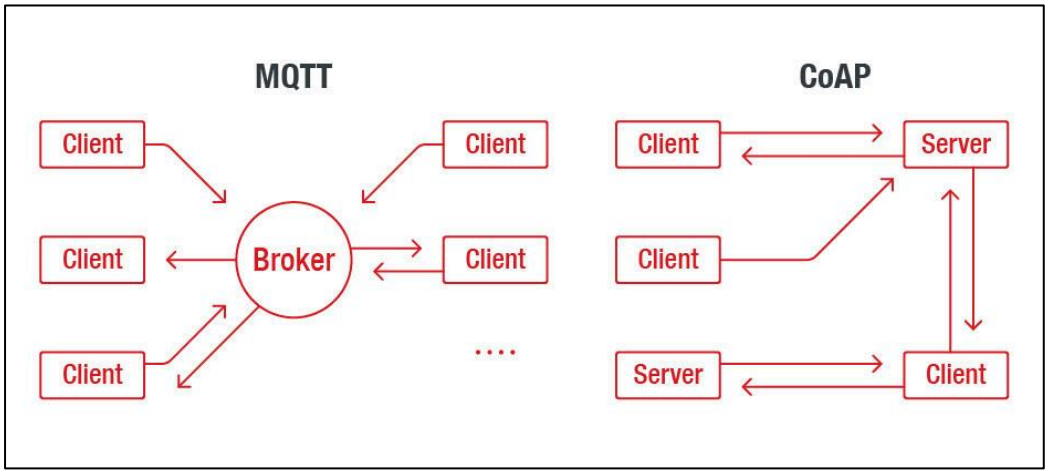
IoT attack surface or spots where threats and vulnerabilities may exist in IoT systems and applications include;

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

Communication Channels

Attacks may emanate through the channels that link different IoT components together through different protocols. IoT system protocols may have security issues that affect the system as a whole. Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) are two of the protocols that Internet of Things devices use to communicate with one another.

Figure 1: **View of the Interaction models of MQTT and CoAP Source (Maggi, Vosseler, & Quarta, 2018)**



Publish-subscribe protocol called MQTT enables broker-mediated one-to-many connectivity. Clients can subscribe to a broker to receive specific messages or publish messages to a broker. Topics, which are effective "tags" that serve as a method for distributing messages to subscribers, are used to arrange messages. In contrast to MQTT, CoAP is a client-server protocol that is not yet standardised. A client node can provide commands to another node using CoAP by transmitting a CoAP packet. In accordance with its logic, the CoAP server will interpret it, extract the payload, and take appropriate action. The request does not always need to be acknowledged by the server (Chaudhary, Peddoju, & Kadarla, 2017).

MQTT is preferred over CoAP for mission-critical communications because it can impose quality of service requirements and guarantee the delivery of messages, as for gathering telemetry data from transient, low-power nodes such as tiny field sensors, CoAP is favoured (Sharma & Nandal, 2020).

Between 2016 and 2017, IOActive's Lucas Lundgren conducted an internet-wide scan of open MQTT endpoints, which revealed an apparent deployment issue among tens of thousands of insecure MQTT hosts (Brad, 2017). Smart home-centric MQTT AVAST's research highlighted the lack of secure configurations and the likelihood of configuration errors in MQTT-enabled home devices (Hron, 2018). The fact that you can view the MQTT server and all the messages passing across it makes the MQTT configuration error worse. More troubling is the fact that many MQTT servers with poor configuration are also freely accessible online without a password, giving cybercriminals access to any home using them.

If the server is publicly accessible, the cybercriminal has the "advantage" of being able to connect to it from any location. Additionally, because the majority of users do not set up access controls in the form of Access Control Lists (ACLs) when configuring a Mosquitto while setting up their smart home hub, cybercriminals can not only subscribe to the server but can also publish to it, taking control of all the devices in a smart home (Anthraper & Kotak, 2019).

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

With such challenges in communication channels, the endpoints within the 5G network, which are the devices, the vulnerable endpoints can disclose records and leak data for unauthorised access, some of which we discovered to be tied to crucial industries. Denial-of-service (DoS) assaults on vulnerable endpoints are another possibility, as is the possibility that they will be exploited to take complete control.

Devices

Devices might be the primary means of starting an attack. A device may have vulnerabilities in its memory, firmware, physical interface, web interface, and network services, for example. Insecure default settings, outdated components, and insecure update mechanisms may potentially be advantageous to attackers.

The security flaws in IoT firmware are said to pose a danger to the Internet infrastructure in recent large-scale attacks (He et al., 2021). The firmware running on IoT devices typically contains several security vulnerabilities, such as perilous open ports and hard coding problems, since IoT product providers lack security awareness which makes IoT devices prone to attacks. These assaults range from creating a network of embedded devices similar to the Mirai botnet to several firmware flaws that can be exploited. For instance, the stack overflow vulnerability CVE-2018-0171, which was discovered in the Cisco IOS Software and Cisco IOS XE Software's Smart Install functionality, might result in remote code execution in Cisco routers. On April 7, 2018, a cyber-attack group called "JHT" used it to attack the network infrastructure in Russia and Iran. ISPs (Internet Service Providers), data centres, and certain websites were also compromised (Antonakakis et al., 2017).

Applications and Software

Systems can become compromised as a result of flaws in IoT device software and online applications. For instance, malicious firmware upgrades or user passwords can be stolen through web applications.

The web, mobile, and cloud interfaces are used to manage and administer a sizable number of IoT products and services. However, many of these web interfaces feature weak and open-to-vulnerability security systems. Plaintext logins and user credentials are typically required for both authentication and authorisation (Sarrab & Alnaeli, 2019).

Due to the vast volume of data utilised online, various vulnerabilities, including fraud and cyber-attacks, have been revealed. Since most networks are controlled by intrusion detection, hackers have been increasingly targeting online applications in recent years (Divyaniyadav, Gupta, Singh, Kumar, & Sharma, 2018). Since most IoT devices are managed through a web application, this forms an attack surface that hackers can use to exploit users' data.

CONCLUSION

Ultimately, a trustworthy data privacy framework for IoT devices should satisfy the urgent requirement to safeguard user privacy in a society that is becoming more and more wired. The framework should strive to build a strong and comprehensive approach to ensuring data privacy by including numerous factors and procedures. IoT devices may offer customers a better level of privacy protection by applying a comprehensive data privacy framework, encouraging confidence in the linked ecosystem, and enabling the safe and responsible use of IoT technology. Network segmentation should be incorporated to enable the devices to have their own dedicated secure networks. This could entail using a special network for IoT devices or reinforcing the network with firewalls and intrusion detection systems. The likelihood and effects of unauthorised access, disclosure, alteration, or destruction of the data should be addressed urgently before it is too late to lose data to cyber predators.

REFERENCE

Ahmad, I. & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine*, *2*(1),

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

36– 43. https://doi.org/10.1109/MCOMSTD.2018.1700063

Anthraper, J. J., & Kotak, J. (2019). Security, Privacy and Forensic Concern of MQTT Protocol. *SSRN Electronic Journal*, *January*. https://doi.org/10.2139/ssrn.3355193

Antonakakis, M. & Zhou, Y. (2017). Understanding the Mirai Botnet. *USENIX Security*, 1093–1110.

Anwar, R. W. & Iqbal, S. (2020). Security Threats and Challenges to IoT and its Applications: A Review. *2020 5th International Conference on Fog and Mobile Edge Computing, FMEC 2020*, 301– 305. https://doi.org/10.1109/FMEC49853.2020.9144832

Aravindhan P, S. C., & Shamir Adleman, R.-R. (2008). Multifactor Authentication in IoT devices for ensuring secure cloud storage in Smart Banking. *International Research Journal of Engineering and Technology*, *9001*, 1307. www.irjet.net

Ateniese, G. & Felici, G. (2015). Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers. *International Journal of Security and Networks*, *10*(3), 137–150. https://doi.org/10.1504/IJSN.2015.071829

Australian Government. (2017). IP Australia and the Future of Intellectual Property Megatrends, scenarios and their strategic implications. July.

Azrour, M. & Kanwal, A. (2021). Internet of Things Security: Challenges and Key Issues. *Security and Communication Networks*, *24*(7), 1951– 1957. https://doi.org/10.1080/09720529.2021.1957189

Balough, C. D. (2011). Privacy implications of smart meters. *Chi.-Kent L. Rev.*, *1*(1), 161–191. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/chknt86&section=10

Brad, M. (2017). Licensed by Sunshine Cracked by: Catania, E., & La Corte, A. (2018). IoT Privacy in 5G Networks. *IoTBDS 2018 - Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security*, *2018-March* (IoTBDS 2018), 123–131. https://doi.org/10.5220/0006710501230131

Chaudhary, A. & Kadarla, K. (2017). Study of Internet-of-Things Messaging Protocols Used for Exchanging Data with External Sources. *Proceedings - 14th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2017*, 666–671. https://doi.org/10.1109/MASS.2017.85

Colquhoun, L. (2022, October 1). *IoT Security Is Giving Healthcare Heart Attacks | CDOTrends*. CDO TRENDS Digital & Data Insights for Business Leaders. https://www.cdotrends.com/story/17594/iot-security-giving-healthcare-heart-attacks

Cybersecurity & Infrastructure Security Agency. (2022). AUTHENTICATION. In *CISA* (Issue January).

Cynerio. (2022). The State of Healthcare IoT Device Security 2022.

Daemen, J., & Rijmen, V. (2000). The block cipher rijndael. *International Conference on Smart Card Research and Advanced Applications*, *1820*, 277–284. https://doi.org/10.1007/10721064_26

Divyaniyadav & Sharma, U. (2018). Vulnerabilities and security of web applications. *2018 4th International Conference on Computing Communication and Automation, ICCCA 2018*, 1– 5. https://doi.org/10.1109/CCAA.2018.8777558

Ducklin, P. (2014). *New York City makes a hash of taxi driver data disclosure – Naked Security*. Nacked Security by SOPHOS. https://nakedsecurity.sophos.com/2014/06/24/new-york-city-makes-a-hash-of-taxi-driver-data-disclosure/

Feng, Y. & Chen, D. (2019). Poster: IoT device discovery and identification using network traffic data. *WiSec 2019 - Proceedings of the*

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

2019 Conference on Security and Privacy in Wireless and Mobile Networks, 338–339. https://doi.org/10.1145/3317549.3326320

Geeng, C., & Roesner, F. (2019). DRAFT: Who's In Control ?: Interactions In Multi-User Smart Homes. *Association For Computing Machinery, Section 4*.

Gibbs, S. (2016, April 19). *SS7 hack explained: what can you do about it? | Hacking | The Guardian*. The Guardian. https://www.theguardian.com/technology/2016/apr/19/ss7-hack-explained-mobile-phone-vulnerability-snooping-texts-calls

Gong-Guo, Z., & Wan, Z. (2021). Blockchain-based IoT security authentication system. *Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021*, 415–418. https://doi.org/10.1109/CBFD52659.2021.00090

Groopman, K. (2018, February 12). *Six challenges facing blockchain and IoT convergence - IoT Agenda*. TechTarget. https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Six-challenges-facing-blockchain-and-IoT-convergence

GSMA. (2019). *Protecting Privacy and data in the Internet of things* (Issue February). https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

Haris, R. M., & Al-Maadeed, S. (2020). Integrating Blockchain Technology in 5G enabled IoT: A Review. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, 367– 371. https://doi.org/10.1109/ICIoT48696.2020.9089600

Haus, M. & Member, S. (2017). Security and Privacy in Device-to-Device (D2D) Communication : A Review. 19(2), 1054–1079.

He, D. & Guizani, N. (2021). Toward Hybrid Static-Dynamic Detection of Vulnerabilities in IoT Firmware. *IEEE Network*, *35*(2), 202–207. https://doi.org/10.1109/MNET.011.2000450

Hewa, T. M. & Liyanage, M. (2020). Blockchain for 5G and IoT: Opportunities and Challenges. *2020 8th International Conference on Communications and Networking, ComNet2020 - Proceedings*. https://doi.org/10.1109/ComNet47917.2020.9306082

Hron, M. (2018, August 16). *Are smart homes vulnerable to hacking?* AVAST. https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes

Jafarnia-Jahromi, A. & Lachapelle, G. (2012). GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, *2012*. https://doi.org/10.1155/2012/127072

Johnson, M. E. & Willey, N. D. (2016). The Security Risks of Peer-to-Peer File Sharing Networks. Centre for Digital Strategies Tuck School of Business Dartmouth College, Https://Citeseerx.Ist.Psu.Edu.

Kar, U. N., & Sanyal, D. K. (2020). A Critical Review of 3GPP Standardization of Device-to-Device Communication in Cellular Networks. *SN Computer Science*, *1*(1). https://doi.org/10.1007/s42979-019-0045-5

Katiyar, V. & Gupta, S. (2010). A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment. *International Journal of Computer Applications*, *11*(10), 41–46. https://doi.org/10.5120/1615-2171

Krishnan, H. (2023, March 31). *Security challenges associated with healthcare IoT devices*. Log360. https://www.manageengine.com/log-management/cyber-security/security-issues-healthcare-iot-devices.html

Kumar, B. R. & Naidu, G. A. (2015). An ElGamal Encryption Scheme of Adjacency Matrix and

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

Finite Machines. *Compusoft*, *4*(3), 1548–1554.

Landerreche, E., & Stevens, M. (2018). On Immutability of Blockchains. *Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET)*, 1–8. https://doi.org/10.18420/blockchain2018

Lu, C., & Tseng, S. (2002). Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter. *Proceedings of the International Conference on Application-Specific Systems, Architectures and Processors*, 277–285. https://doi.org/10.1109/ASAP.2002.1030726

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Magalakshmi, V. B., & Kumar, D. S. (2017). Privacy Protection and Authentication Handover in 4G Network : A Survey of Literature. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(6), 32–37.

Maggi, F. & Quarta, D. (2018). The fragility of industrial IoT's data backbone. *Trend Micro Inc.*, 1–65.

Meneghello, F. & Zanella, A. (2019). IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*, *6*(5), 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189

Mohammed, H. & Awwad, F. (2020). Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks. *IEEE Access*, *8*, 36847–36862. https://doi.org/10.1109/ACCESS.2020.2975016

Mohanta, B. K. & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*, 10–13. https://doi.org/10.1109/ICCCNT.2018.8494045

National Institute of Standards and Technology. (2010). Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid. *National Institute of Standards and Technology*, *2*(August), 69. http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf

National Security Agency. (2021). *Potential threat vectors to 5G infrastructure*. 1–16. https://media.defense.gov/2021/May/10/2002637751/-1/-1/1/POTENTIAL THREAT VECTORS TO 5G INFRASTRUCTURE.PDF

Nechvatal, J. & Roback, E. (2001). Report on the Development of the Advanced Encryption Standard (AES). *Journal of Research of the National Institute of Standards and Technology*, *106*(3), 511. https://doi.org/10.6028/JRES.106.023

Nyemba, chisomo. (2019). Right to Data Privacy in the Digital Era Critical Assessment of Malawi's Data.

Office of the Australian Information Commissioner. (2016, September 23). *Privacy Commissioners reveal the hidden risks of the Internet of Things - Home*. https://www.oaic.gov.au/updates/news-and-media/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things

Office of the Victorian Information Commissioner. (2021). *Internet of things and privacy issues and challenges*. *April*. https://doi.org/10.33965/es2021_202101r046

Palo Alto Networks. (2020). 2020 Unit 42 IoT Threat Report. In *Paloaltonetworks.Com*. https://drive.google.com/open?id=1VLA1IweXyJMVeWxvy_8vwtypUQXB_Uhn

Panicker, J. G. & Rudolph, C. (2021). Authentication and Access Control in 5G

Article DOI: https://doi.org/10.37284/eajit.6.1.1333

Device-to-Device Communication. Proceedings - 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2021, 1575–1582. https://doi.org/10.1109/TrustCom53373.2021.00229

Peppet, S. R. (2014). Regulating the Internet of things: First steps toward managing discrimination, Privacy, Security, And consent. *Texas Law Review*, *93*(1), 85–179.

Qian, Y. & Pustišek, M. (2018). Towards decentralised IoT security enhancement: A blockchain approach. *Computers and Electrical Engineering*, *72*, 266– 273. https://doi.org/10.1016/j.compeleceng.2018.08.021

Rajagopalan, S. R. & Poor, H. V. (2011). Smart meter privacy: A utility-privacy framework. *2011 IEEE International Conference on Smart Grid Communications, SmartGridComm 2011*, 190–195. https://doi.org/10.1109/SmartGridComm.2011.6102315

Rghioi, A. & Bouhorma, M. (2014). Security Review and Proposed Solution. *Ieee*, 384–389.

Sarma, A. C., & Girão, J. (2009). Identities in the future Internet of things. *Wireless Personal Communications*, *49*(3), 353–363. https://doi.org/10.1007/s11277-009-9697-0

Sarrab, M., & Alnaeli, S. M. (2019). Critical Aspects Pertaining Security of IoT Application-Level Software Systems. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, 960– 964. https://doi.org/10.1109/IEMCON.2018.8614993

Shacklett, M. (2021, November). *What is multifactor authentication (MFA) and how does it work?* SearchSecurity. https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Sharma, A., & Nandal, V. (2020). Comparison between the Messaging Protocols : CoAP and MQTT Protocol. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *7*(7).

Sicari, S. & Coen-Porisini, A. (2020). 5G In the Internet of things era: An overview on security and privacy challenges. *Computer Networks*, *79*(June). https://doi.org/10.1016/j.comnet.2020.107345

Singh, A. & Mukhopadhyay, S. (2019). Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes. *IEEE Internet of Things Journal*, *6*(1), 421–434. https://doi.org/10.1109/JIOT.2018.2861324

Singh, G. P., & Bangotra, P. K. (2021). Internet of Things (IoT): Vulnerability, Attacks, and Security. *Wireless Sensor Networks and the Internet of Things*, *July*, 247–262. https://doi.org/10.1201/9781003131229-19

Tiburski, R. T. & Hessel, F. (2016). Security challenges in 5G-based iot middleware systems. *Modeling and Optimisation in Science and Technologies*, *8*(April), 399–418. https://doi.org/10.1007/978-3-319-30913-2_17

Tushnet, M. V. (2009). In the matter of Nomi Technologies, Inc (United States of America Before the Federal Trade Commission, Docket No. C-4538, August 28 2015). In *The "Militant Democracy" Principle in Modern Democracies*.

Van, D. H., & Thuc, N. D. (2015). A privacy preserving message authentication code. *2015 5th International Conference on IT Convergence and Security, ICITCS 2015 - Proceedings*, *1*, 15– 18. https://doi.org/10.1109/ICITCS.2015.7292927

Wazid, M. & Rodrigues, J. J. P. C. (2020). Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap. *IEEE Access*, *8*, 1– 25. https://doi.org/10.1109/ACCESS.2020.3047895

