International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 6, Nov-Dec-2019, ISSN (Online): 2395-566X

Energy Sector Applications: Nanomaterials in Batteries and Solar Cells

Dr. Zainal Shareif
Universiti Sains Malaysia

Abstract- The growing global demand for energy, coupled with the urgent need to transition to sustainable sources, has intensified interest in advanced technologies that can enhance energy generation and storage. Nanomaterials, with their unique physicochemical properties at the nanoscale, are playing a transformative role in improving the performance of batteries and solar cells. This paper examines the fundamental mechanisms by which nanomaterials enhance electrical conductivity, charge storage, and energy conversion efficiency. It explores their applications in lithium-ion and next-generation batteries, as well as in various photovoltaic technologies including silicon-based, thin-film, organic, and perovskite solar cells. The paper also discusses environmental and economic considerations, highlighting the need for sustainable synthesis and lifecycle assessments. Looking ahead, it evaluates emerging trends such as AI-driven material discovery and multifunctional nanostructures that promise to shape the future of the energy sector. Through a multidisciplinary lens, this work underscores the critical role of nanotechnology in enabling high-performance, scalable, and environmentally responsible energy solutions.

Keywords – Nanomaterials, Lithium-ion batteries, Solar cells, Energy storage, Photovoltaics, Perovskite, Thin-film technology.

I. INTRODUCTION

The global demand for energy continues to rise sharply, driven by rapid industrialization, expanding urban landscapes, and an ever-growing population. Traditional energy systems, heavily reliant on fossil fuels, are increasingly unsustainable due to their environmental impact and finite availability. The dual pressures of depleting resources and intensifying climate change have accelerated the global pursuit of renewable and sustainable energy alternatives. Among the most promising solutions in this green transition are solar power generation and advanced energy storage technologies, particularly batteries. However, conventional solar cells and battery systems often face significant limitations, including low energy conversion efficiency, high production costs, and limited material sustainability.

Nanotechnology emerges as a transformative solution to address these barriers. By manipulating matter at the nanometer scale, scientists and engineers can design materials with tailored electronic, thermal, and mechanical properties that outperform their bulk counterparts. Nanomaterials exhibit exceptional characteristics such as increased surface area, quantum confinement effects, and enhanced electrical and thermal conductivity. These properties are particularly advantageous in improving the performance, durability, and affordability of both solar cells and battery systems. For example, in maintaining ecology, by remediating contaminants, nanostructured electrodes in lithium-ion batteries can significantly boost charge storage capacity and cycling stability, while nanoscale light-absorbing layers in solar cells can enhance photon capture and conversion efficiency [1-5].

This paper provides a comprehensive examination of how nanomaterials are revolutionizing energy systems, focusing on their roles in batteries and solar cells. It focuses into the underlying mechanisms of their enhanced performance, recent advancements in nanomaterial applications, and the environmental and economic implications of their widespread adoption. Furthermore, it outlines the current challenges and future research directions needed to fully harness nanotechnology's potential. By synthesizing insights across disciplines, the study underscores the pivotal role of nanomaterials in driving innovation and fostering a more sustainable, resilient global energy infrastructure.

II. FUNDAMENTALS OF NANOMATERIALS IN ENERGY SYSTEMS

Nanomaterials are materials engineered at the nanoscale (typically 1-100 nm) that exhibit unique physical and chemical properties due to their size, shape, and surface characteristics. In energy systems, these materials are utilized to enhance conductivity, reactivity, strength, and optical absorption, which are critical for improving battery and solar cell performance. For instance, nanoparticles, nanowires,

© 2019 IJSRET

nanotubes, and quantum dots provide increased surface area, which is essential for catalysis and electrochemical reactions.

Their quantum mechanical behaviors also allow for novel electron transport pathways, enabling faster and more efficient energy conversion and storage. In batteries, nanostructured materials facilitate rapid ion diffusion and stable electrode interfaces, thus extending lifespan and performance. In solar cells, nanoscale architectures improve light absorption, charge separation, and carrier mobility, which collectively increase efficiency.

Materials such as graphene, carbon nanotubes, metal oxides, and perovskites are at the forefront of nanotechnology applications. The synergy between nanostructure design and functional performance lies at the heart of these advancements. Understanding the interaction between nanomaterials and their operational environments, including stability under thermal and electrochemical stress, is crucial for developing next-generation energy solutions. Thus, a fundamental grasp of nanoscale phenomena provides the foundation for innovating high-performance, cost-effective, and sustainable energy technologies [1-5].

III. NANOMATERIALS IN BATTERY TECHNOLOGIES

1. Lithium-Ion Batteries

Lithium-ion batteries (LIBs) are the dominant energy storage technology powering everything from smartphones to electric vehicles. Yet, conventional LIBs face limitations such as limited capacity, thermal instability, and degradation over repeated cycles.

Nanomaterials offer transformative solutions to these challenges. Nanoscale materials used in LIB anodes (like silicon nanoparticles and graphene) provide higher specific capacities compared to traditional graphite. Their large surface area facilitates fast lithium-ion diffusion and improved charge/discharge rates. Similarly, cathode materials like lithium iron phosphate (LiFePO4) benefit from nanostructuring to enhance conductivity and cycle life.

Nanocoatings can stabilize interfaces and prevent the formation of detrimental solid-electrolyte interphases. Moreover, conductive nanomaterials improve electron transport, reduce internal resistance, and enable flexible battery designs. However, integrating nanomaterials into LIBs also presents challenges, such as maintaining structural integrity, avoiding agglomeration, and managing cost-effective large-scale production. Innovative fabrication techniques, such as atomic layer deposition and electrospinning, are being developed to address these concerns. Overall, nanomaterials significantly improve energy density, rate capability, and operational safety, positioning LIBs for broader application in grid storage and electric transportation [5-7].

2 Beyond Lithium-Ion

The quest for sustainable and high-performance energy storage is pushing research beyond conventional lithium-ion batteries. Emerging systems such as sodium-ion, lithium-sulfur, and solid-state batteries stand to benefit immensely from nanotechnology.

Sodium-ion batteries, which use abundant and inexpensive materials, often suffer from sluggish ion diffusion and lower energy density. Nanoscale electrode materials like layered metal oxides and carbon nanocomposites enhance ion transport and stability. Lithium-sulfur batteries, with their high theoretical energy density, face challenges like polysulfide dissolution and poor conductivity. Nanostructured sulfur hosts, porous carbon matrices, and nanoscale encapsulation techniques address these issues, promoting longer cycle life and higher capacity.

In solid-state batteries, which replace flammable liquid electrolytes with solid alternatives, nanomaterials enable better ionic conductivity and interface compatibility. For instance, nanoparticle-infused solid electrolytes enhance mechanical flexibility and suppress dendrite formation. These advances are critical for enabling safer, more efficient, and longer-lasting energy storage solutions. As research continues, nanotechnology will be instrumental in bridging the gap between laboratory prototypes and commercial-scale energy storage systems, ecological diversity imbalances [7-9].

IV. NANOMATERIALS IN SOLAR CELLS

1. Silicon-Based Solar Cells

Silicon-based photovoltaic (PV) cells dominate the global solar energy market due to their proven performance and reliability. However, their efficiency is constrained by physical and optical limitations such as surface reflection and limited absorption in certain wavelengths. Nanotechnology addresses these challenges by enhancing light management and carrier collection. For example, nanostructured antireflective coatings, including silicon nanowires and nano-patterned surfaces, reduce reflectivity and increase photon capture. Additionally, plasmonic nanoparticles (e.g., silver or gold) embedded in the solar cell structure can concentrate light through localized surface plasmon resonance, further boosting efficiency.

© 2019 IJSRET

Nanoporous silicon layers and quantum dots can also be integrated to extend the absorption spectrum and tailor bandgaps.

These innovations not only improve power conversion efficiency but also allow for thinner, lighter, and more flexible solar cells. Furthermore, nanomaterials contribute to thermal management and enhance mechanical stability under environmental stress. Although integrating these nanoscale enhancements into commercial production remains challenging, ongoing advances in fabrication methods such as nanoimprint lithography and self-assembly are making such improvements increasingly viable for industrial deployment [9-11].

2. Thin-Film and Organic Solar Cells

Thin-film and organic photovoltaic (OPV) technologies offer lightweight, flexible, and potentially lower-cost alternatives to traditional silicon solar cells. However, their broader adoption has been hampered by lower efficiency and stability. Nanomaterials are pivotal in overcoming these limitations.

In thin-film solar cells, nanostructured materials such as cadmium telluride (CdTe) and copper indium gallium selenide (CIGS) enhance light absorption and charge collection due to their superior morphology and optoelectronic properties. In OPVs, the incorporation of carbon-based nanomaterials like graphene and carbon nanotubes improves electron mobility and mechanical strength.

Moreover, the use of nanostructured donor-acceptor interfaces enhances exciton dissociation and charge transport efficiency. Quantum dots and metal oxide nanoparticles also play critical roles in extending absorption spectra and stabilizing device architectures. These advances enable the development of semi-transparent and wearable solar panels suited for building-integrated and portable applications. While environmental concerns and scalability of some nanomaterials remain, the continuous evolution of green synthesis methods and inkjet printing technologies promises to address these challenges, paving the way for commercially viable thin-film and organic solar cells [8-13].

3. Perovskite Solar Cells

Perovskite solar cells have emerged as a groundbreaking technology, offering high efficiency with low manufacturing costs. The inclusion of nanomaterials has significantly enhanced their performance and stability. Nanocrystalline perovskite layers exhibit superior light-harvesting properties, while nanoparticles and 2D nanomaterials such as graphene and MXenes improve electron transport and reduce recombination losses. Additionally, incorporating nanomaterials into transport layers and electrode interfaces boosts conductivity and structural integrity. Encapsulation with nanocomposite barriers also extends device lifetimes by protecting against moisture and oxygen degradation. Despite these advances, perovskite solar cells face challenges like lead toxicity, long-term operational stability, and upscaling. Researchers are exploring lead-free alternatives and hybrid nanostructures to address these concerns. The integration of perovskite layers into tandem cell architectures, where they complement silicon or other PV materials, further amplifies overall efficiency. With the aid of nanotechnology, perovskite solar cells are approaching commercial viability, offering the potential to disrupt the photovoltaic market by combining high efficiency with low-cost, solution-based manufacturing processes [8-13].

V. ENVIRONMENTAL AND ECONOMIC CONSIDERATIONS

The deployment of nanomaterials in energy technologies offers clear performance benefits, but it also raises environmental and economic concerns. The lifecycle assessment (LCA) of nanomaterials, from raw material extraction to disposal, is essential to ensure sustainability. Some nanomaterials, such as heavy metals or non-biodegradable compounds, may pose ecological and human health risks if not properly managed.

Safe synthesis methods, green chemistry principles, and biodegradable nanomaterials are therefore gaining attention. Economically, the high cost of precision manufacturing, quality control, and scalability remains a barrier to widespread adoption. Nonetheless, ongoing innovations in low-cost production techniques, such as roll-to-roll processing and solution-phase synthesis, are improving cost-efficiency.

Additionally, nanomaterials can extend the lifespan of devices, reduce energy consumption, and enhance recycling potential, contributing to circular economy principles. Policymakers, manufacturers, and researchers must collaborate to establish clear regulatory frameworks and standardized testing protocols for nanomaterial safety and performance. Transparent communication with stakeholders and end-users is also critical to build public trust. Ultimately, balancing innovation with responsible development ensures that nanotechnology fulfills its promise in building a sustainable energy future [8-13].

VI. FUTURE PERSPECTIVES AND EMERGING TRENDS

© 2019 IJSRET

The future of nanomaterials in energy systems is promising, driven by rapid advancements in materials science, data analytics, and engineering. Integrating artificial intelligence (AI) and machine learning in nanomaterial design accelerates the discovery of optimal compositions and structures for specific applications. Furthermore, coupling nanotechnology with the Internet of Things (IoT) enables smart energy systems with real-time monitoring and adaptive performance.

Hybrid energy systems that combine solar cells and batteries at the nanoscale offer seamless energy generation and storage solutions. Research is also focusing on multi-functional nanomaterials that can harvest energy from multiple sources (e.g., light, heat, and mechanical stress) simultaneously. The rise of biodegradable and bio-inspired nanomaterials addresses growing environmental concerns. Innovations in 3D nanostructuring and additive manufacturing further open new pathways for designing customized, high-performance energy devices.

Meanwhile, policy support, international collaboration, and public-private partnerships are crucial to translating laboratory research into market-ready technologies. Education and workforce training in nano-energy technologies will also play a vital role in scaling innovation. As the energy sector evolves, nanotechnology will remain a central driver of sustainable and decentralized energy solutions [8-13].

VII. CONCLUSION

Nanotechnology is redefining the landscape of energy generation and storage by unlocking new potentials in batteries and solar cells. Through the strategic use of nanomaterials, energy devices become more efficient, compact, and adaptable to diverse applications.

In batteries, nanoscale engineering enhances charge capacity, rate performance, and safety, extending the range and lifespan of energy storage systems. In solar cells, nanomaterials improve light absorption, charge transport, and structural stability, leading to higher energy conversion efficiencies. Despite these benefits, challenges remain in terms of environmental impact, cost, and manufacturability.

Addressing these concerns requires interdisciplinary collaboration, responsible innovation, and supportive policy frameworks. The integration of emerging technologies such as AI, IoT, and green chemistry with nanotechnology will further amplify its impact. As we strive toward carbon neutrality and energy resilience, nanomaterials stand out as enablers of the next-generation energy infrastructure. By fostering innovation while ensuring sustainability, nanotechnology can catalyze a cleaner, smarter, and more equitable global energy future.

REFERENCE

1. Chinthala, L. K. (2018). Environmental biotechnology: Microbial approaches for pollution remediation and resource recovery. In Ecocraft: Microbial Innovations (Vol. 1, pp. 49–58). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5232415
2. Baker S, Satish S (2015) Biosynthesis of gold nanoparticles by Pseudomonas veronii AS41G inhabiting Annona squamosa L. Spectrochim Acta A Mol Biomol Spectrosc 150:691–695
3. Chinthala, L. K. (2013). Advancements in microbial technologies for environmental management. In Microbes and Ecosystem (Vol. 1, pp. 20–28). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5231963
4. Orilall, M.C., & Wiesner, U.B. (2011). Block copolymer based composition and morphology control in nanostructured hybrid materials for energy conversion and storage: solar cells, batteries, and fuel cells. Chemical Society reviews, 40 2, 520-35 .
5. Dai, L., Chang, D.W., Baek, J., & Lu, W. (2012). Carbon nanomaterials for advanced energy conversion and storage. Small, 8 8, 1130-66 .
6. Cao, X., Tan, C., Zhang, X., Zhao, W., & Zhang, H. (2016). Solution-Processed Two-Dimensional Metal Dichalcogenide-Based Nanomaterials for Energy Storage and Conversion. Advanced Materials, 28.
7. Li, F., Ran, J., Jaroniec, M., & Qiao, S. (2015). Solution combustion synthesis of metal oxide nanomaterials for energy storage and conversion. Nanoscale, 7 42, 17590-610 .
8. Cheekati, S.L., Xing, Y., Zhuang, Y., & Huang, H. (2010). Nanographene Platelets and Their Composites for Li-Ion Batteries.
9. Chinthala, L. K. (2016). Environmental microbiomes: Exploring the depths of microbial diversity. In Microbial Ecology: Shaping the Environment (Vol. 2, pp. 1–12). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5232403
10. Graetzel, M. (1996). Nanocrystalline oxide films : Nanomaterials. Analusis, 24.
11. Park, H.S., Choi, B.G., Yang, S.H., Shin, W.H., Kang, J.K., Jung, D., & Hong, W.H. (2009). Ionic-liquid-assisted sonochemical synthesis of carbon-nanotube-based nanohybrids: control in the structures and interfacial characteristics. Small, 5 15, 1754-60 .
12. Raffaelle, R.P., Landi, B.J., Elich, J.B., Gennett, T., Castro, S.L., Bailey, S.G., & Hepp, A.F. (2003).

© 2019 IJSRET

Nanostructured Materials Development for Space Power.
13. Service, R.F. (2008). Can High-Speed Tests Sort Out Which Nanomaterials Are Safe? Science, 321, 1036 - 1037.

In the short time that social networks have been around, experience has shown that publishing the entire content on Facebook and Google+, along with an eye-catching photo and a link to the original content, helps the audience to learn about the content, consume it and, if they like it, share the content for others to access [4]. The importance of this new system of communication with the audience is such that several websites, including Buzzfeed and Upworthy, have built their business around riding the wave of social networks [5]. The volume and type of content on these websites is optimized for consumption and reposting on social networks, and the technical structure of these environments is designed in such a way that after watching a video and reading a text, the user is offered options to share on social networks. The important point is that the attractive appearance of social networks and the sea of possibilities they offer for social activity should not lead to an emotional and unconsidered approach to them. The truth is that these wonderful phenomena are still evolving and changing, and many aspects of activity on social networks still remain unknown [6]. The transfer of social activity from the physical environment to the virtual and interactive world of social networks is an event that has a substantial impact on the characteristics of social activity and active communication with its audience. To have a successful presence on social networks, one must analyze these effects and be aware of their presence [7].

Although social networks offer privacy settings, these settings should not be relied upon for sensitive matters. Various social networks have shown that the details of privacy settings change over time and users do not have the opportunity to update their privacy with these changes. In addition, various Internet tools have become vulnerable to attacks or coding and configuration errors over time. As a general rule, sensitive and confidential information should not be provided not only on social networks, but also on the Internet [8].

Based on the privacy policy, service providers and users agree on what information about them will be displayed or used in any way. If in any other way, outside the confidentiality agreement, user information is misused, users will have the opportunity to file a lawsuit and file a complaint against the service provider website. Usually, in social networks, even the most detailed user information can be received and published. Interests, education, family connections, friendships, occupation, location, school, and birthplace, and many other details are asked. Some social networking sites even ask for hair color, eye color, and height [9].

According to Comscore, social networking sites such as Facebook and Twitter have 84% of the world's online population.[10] Today, with the dramatic advancement of smartphones and internet networks, social networks have become more accessible to smartphone users who can receive news and messages from friends and family.

The convergence of social networks, the advancement of smartphones, and the stability of internet network infrastructures have brought about a pervasive and powerful social network that has helped us to have a stable connection on mobile social networks (MSN) better than ever.

The boom in mobile applications is one of the important factors in the development of mobile social networks. According to Wiki, Apple has increased the number of its mobile applications from 800 in July 2008 to 825,000 in April 2013 [11]. Generally, mobile applications can be divided into three categories [12]. The first category is online social applications (OSA) 4, which enable users to update their profiles, share their photos, and watch online videos on their phones. This relationship is formed by smartphone users (SUs) and Internet service providers (ISPs). The second category is location-based applications. These applications use the Internet to obtain location- based information, which is used by very powerful social networks such as Facebook, Foursquare, and Loopt. The basic idea behind these applications is as follows: The GPS chip detects the location information of smartphone users and reports it to the Internet service providers so that it can be downloaded for location information. The third category of autonomous mobile applications is where smartphone users can communicate with neighboring smartphone users and local service providers using short-range wireless communications such as NFC, Bluetooth, and Wi-Fi Direct [13]. In all three of the above cases, privacy and security are important issues that are addressed in this research.

© 2019 IJSRET

II. THEORETICAL FOUNDATIONS AND RESEARCH BACKGROUND

Virtual social networks are a new generation of social relations space that, despite not being very old, have managed to make a good place in people's lives. Many people of different ages and from different social groups have come together in virtual social networks and communicate with each other from great distances in the real world through social networks. Social networks play a prominent role in today's world and cannot be ignored [14]. These sites affect various aspects of individual and social life of individuals and at the level of countries and even internationally, and for this reason they are expanding and will play a much greater and more important role in life in the future. Virtual social networks are a new generation of Internet websites [15]. On these websites, Internet users gather around a common axis virtually and form online communities. In fact, a social network is a network consisting of individuals and groups and the connections between them [16].

A social network is a site or collection of sites that allows users who are interested in sharing their interests, thoughts, and activities with others. While social networks are a space to find new friends, they also allow people to connect with old friends. They are also places for exchanging ideas, where people share their opinions and views [17].

Social networks are generally places in the virtual world where people briefly introduce themselves and provide the elements of communication between themselves and their like-minded people in various fields of interest. In fact, it is a new form of communication and sharing content on the Internet. Social networks are new platforms that are at the center of attention of Internet users, each of which brings together a group of users with specific characteristics [18]. The friend-making process in many mobile social networks allows users to request a friend connection from users who are geographically nearby or from users who share common interests. But what is important in this issue is how to secure and defend personal information against profit-seeking individuals. For this reason, in this section, most of the profile matching profiles will be reviewed and the latest security approach that has been applied to this process will be introduced [19-20]. To prevent this issue, the Fairness-Aware and Collusion-free Matching algorithm, which is based on Blind Linear Transformation, is used [21,22].

Nyoni and Velempini (2013) examine the privacy issues users are exposed to when using social networks such as Facebook. With the risks of disclosing personal information online, users need to be made aware of what policies and legal instruments exist to cover them. The result of this would be a safer social network experience for all those who use it the most [23].

Liang et al. (2014) examine the architecture, communication patterns, and especially the security and privacy of MSN. We first study three categories of mobile applications with a focus on two autonomous mobile applications, business card and service review. We then explore the possible methods to deal with the associated security and privacy challenges. By discussing the shortages of the methods, we finally provide several promising research directions [24].

III. PROPOSED ALGORITHM

To begin examining and fully understanding the protocol, the protocol must first be implemented to become familiar with all aspects of the protocol. The text of the article mentioned that this protocol was implemented using the Java programming language on a laptop with an Intel core i3- 330 (201GHz) processor and 2 Gb memory. To improve this protocol, it is necessary to re- implement the protocol using the existing algorithms mentioned in the article. For this reason, the protocol was re-implemented using the Java programming language in the Netbeans 8.0.2 environment.

The implementation of this protocol includes four algorithms, including a fast variant of paillier encryption algorithm, which is called and used in three other algorithms. The encryption algorithm will be discussed in detail later in the section.

The Blind Transformation algorithm is the next algorithm to be implemented. This algorithm can be seen in the figure below:

© 2019 IJSRET

Algorithm 1 The Blind Transformation Algorithm

Input: $\mathbb{P}'_a \leftarrow U_a$'s profile encrypted under his public key pk_a, $\mathbb{I}_b \leftarrow U_b$'s interest, $e_b \leftarrow$ the number of interest U_b considers in $\mathbb{I}_b$ and $l_b \leftarrow$ a security parameter.

Output: $\mathbb{P}''_a \leftarrow$ the blind-transformed profile vector for U_a, $\mathbb{I}''_b \leftarrow$ the transformed interest vector for U_b and $s_b \leftarrow$ the actual matching result for U_b.

function BLIND-TRANSFORMATION($\mathbb{P}'_a$, pk_a, $\mathbb{I}_b$, e_b, l_b)
- $r_b \leftarrow$ random vector of length $n = ||\mathbb{P}'_a||$
- $\widetilde{r'_b} \leftarrow \texttt{Encrypt}(r_b, pk_a)$
- $\widetilde{\mathbb{P}_a} \leftarrow \texttt{VecAdd}(\mathbb{P}'_a, r'_b)$
- $\widetilde{\mathbb{I}_b} \leftarrow \texttt{VecAdd}(\mathbb{I}_b, r_b)$
- $y_b \leftarrow$ random vector of length l_b
- $\widetilde{y'_b} \leftarrow \texttt{Encrypt}(y_b, pk_a)$
- $\widetilde{\mathbb{P}'_a} \leftarrow \texttt{VecExt}(\widetilde{\mathbb{P}_a}, y'_b)$
- $k_b \leftarrow$ random number between $[1, l_b]$
- $\widetilde{y_b} \leftarrow \texttt{VecRev}(\widetilde{y_b}, k_b)$
- $\widetilde{\mathbb{I}'_b} \leftarrow \texttt{VecExt}(\widetilde{\mathbb{I}_b}, \widetilde{y_b})$
- $\widetilde{\mathbb{I}''_b} \leftarrow \texttt{VecShuffle}(\widetilde{\mathbb{I}'_b})$
- $\widetilde{\mathbb{P}''_a} \leftarrow \texttt{VecShuffle}(\widetilde{\mathbb{P}'_a})$
- $s_b \leftarrow e_b + l_b - k_b$
- **return** $\mathbb{P}''_a, \mathbb{I}''_b, s_b$

end function

Figure 1: Blind transformation algorithm [25]

As can be seen in the figure, in this protocol, each participant encrypts his profile with the public key and sends it to his partner to execute the protocol.

To explain the protocol more clearly, suppose we have two users Ua and Ub. Initially, user A encrypts his profile with the public key (Pa, pka) and sends it to user B. User B performs the following activities, which include four operations: BlindAdd), Blind Append, Blind Reverse, and Blind Shuffle.

After coding and implementing all 4 algorithms and the entire protocol, its execution is performed in such a way that the number of iterations of the algorithm execution is set in any number of interests and the size of the security parameter can be adjusted. As the programmer of the original article, 21 iterations were considered.

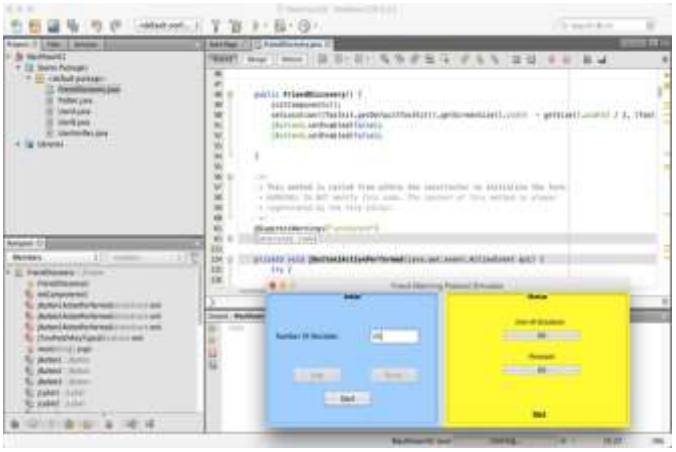

Figure 2: Protocol programming environment in Java

In this research, the key length of the encryption algorithm is 1124 bits, which is exactly equal to Paillier and about 9 times the key length of the fast variant of Paillier algorithm, and the execution time of the entire algorithm is about half, which indicates the success of the proposed algorithm.

In the article, the researcher had greatly reduced the key length of the encryption algorithm to make the protocol execution time reasonable. However, since the key length is very effective in cryptographic security, the proposed plan in this research is to have a better algorithm by increasing the key length to have a suitable execution time, which is the RSA algorithm that has replaced the Fast variant of Paillier algorithm.

IV. RESULTS

As mentioned, to improve the execution time of the protocol, the encryption algorithm was improved and the RSA algorithm was replaced by the Fast variant of Paillier algorithm, and it was claimed that the execution time of the protocol will be better than before despite the increase in the key length of the encryption algorithm. In this section, the implementation results have been fully examined.

1. Algorithm - RSA

As mentioned, according to the mentioned article, the RSA algorithm has a great advantage over the Paillier algorithm and this was shown according to various comparisons. But the working of the RSA algorithm is explained below.

In 1976, Whitfield Diff and Martin Hellman, students of Stanford University, invented and registered one of the most

© 2019 IJSRET

practical methods of encoding information. In this method, which is also known as the asymmetric coding method, two keys are used to encode information. (In older methods, a key was used, which was called symmetric coding). They published their paper in a 1976 issue of the IEEE journal Transactions on Information Theory, which soon revolutionized the information hiding industry in the world.

In the paper, to make the protocol execution time reasonable, the length of the encryption algorithm key was greatly reduced. However, since the length of the key is very effective in encryption security, the proposed plan in this research is to have a better algorithm by increasing the length of the key to have a reasonable execution time, which is the RSA algorithm, which has replaced the Fast variant of Paillier.

2. Implementing the protocol with the proposed encryption algorithm

The protocol includes four algorithms, one of which is a cryptographic algorithm, which is called in three algorithms: Blind transformation, fairness-Aware, and Blind linear transformation. All of these algorithms are performed by both users A and B simultaneously and in parallel, but in this research, like the original article, the timer is active in one user, and this is sufficient to measure the execution time.

Also, when implementing the protocol, it is designed in such a way that it is easy to determine the number of iterations of the protocol execution for any number of interests and any size of security parameter. In implementing the protocol, as in the implementation in the main article, the number of iterations is considered to be 21. This protocol has been implemented and executed on a Macbook MD760 laptop with an Intel Corei5-4250 (2.3GHz) processor and 4GB memory in the Netbeans 8.0.2 environment and the Java programming language. The following figure shows examples of the software environment and how the software is designed and executed:

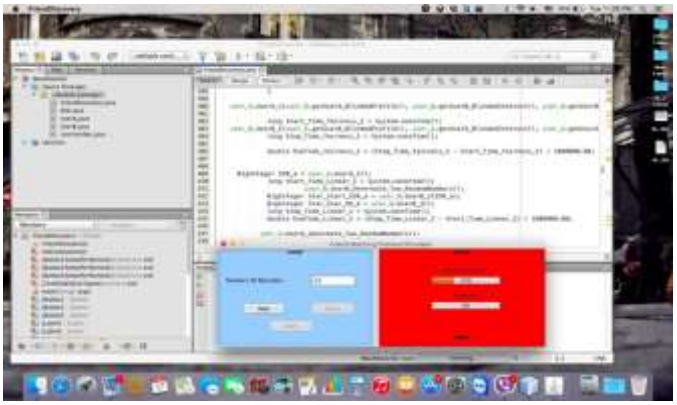

Figure 3: View of the implementation and execution of the protocol

The following figures show the results obtained from the original article and then the implementation of the protocol with the Fast variant of Paillier encryption algorithm that was implemented in the previous section, and then they are compared with the results of implementing the protocol with the proposed RSA encryption algorithm:

Table 1: Results of the Blind Transformation algorithm for different numbers of interests and security parameters (Fast variant of Paillier)

n	I=n	I=2n	I=3n
20	551	834	1100
30	834	1238	1681
40	1122	1647	2217
50	1393	2119	2737
60	1650	2517	3370
70	1973	2911	3957
80	2316	3302	4495
90	2655	3732	5033
100	2973	4234	5550

© 2019 IJSRET

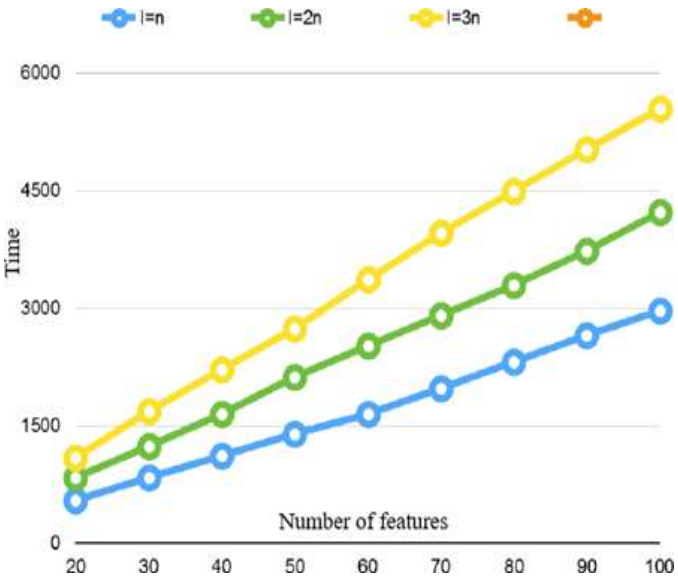

Figure 4: Algorithm execution time graph - Blind Transformation for different number of interests (Fast variant of Paillier)

Figure 4 shows that it increases with increasing security parameter size and also increasing user interests.

Table 2: Algorithm execution time - Blind Transformation for different number of features and security parameter (RSA)

n	I=n	I=2n	I=3n
20	144	210	274
30	210	318	422
40	290	416	578
50	346	526	730
60	428	619	879
70	545	739	1040
80	578	834	1159
90	661	970	1307
100	763	1065	1443

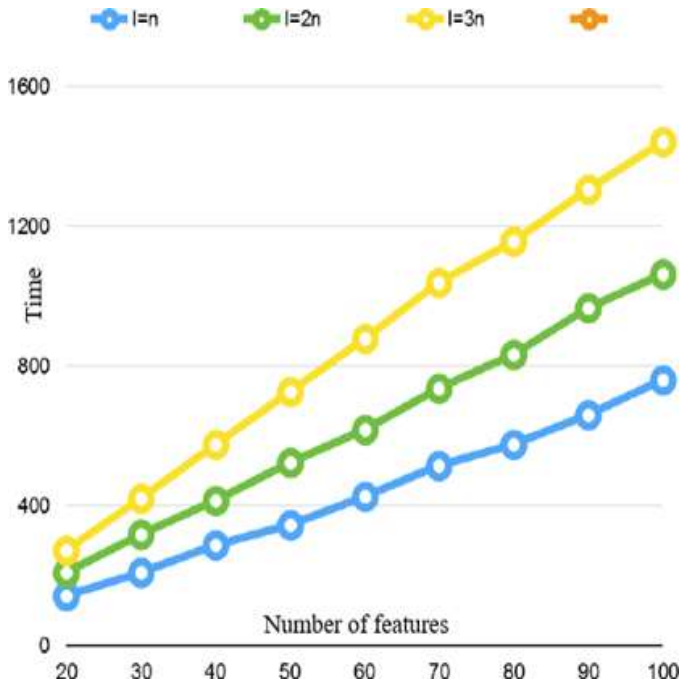

Figure 5: Execution time graph of the algorithm - Blind Transformation for different number of features (RSA)

Figure 5 shows that the majority of the execution time of the protocol depends on the execution time of the algorithm - Blind Transformation and the Encryption operation is the most time- consuming part of the algorithm and increases with increasing security parameter size and increasing user interests. As can be seen, the RSA algorithm, which performs well in the Encryption operation, has significantly reduced the execution time of this algorithm (from 6000 to 1600)

Table 3: Execution time of the algorithm - Fairness_Aware for different number of interests and security parameters (Fast variant of Paillier)

n	I=n	I=2n	I=3n
20	92	138	186
30	140	211	282
40	186	279	374
50	230	360	463
60	283	432	563
70	326	497	669
80	382	567	764

© 2019 IJSRET

90	430	639	839
100	482	716	931

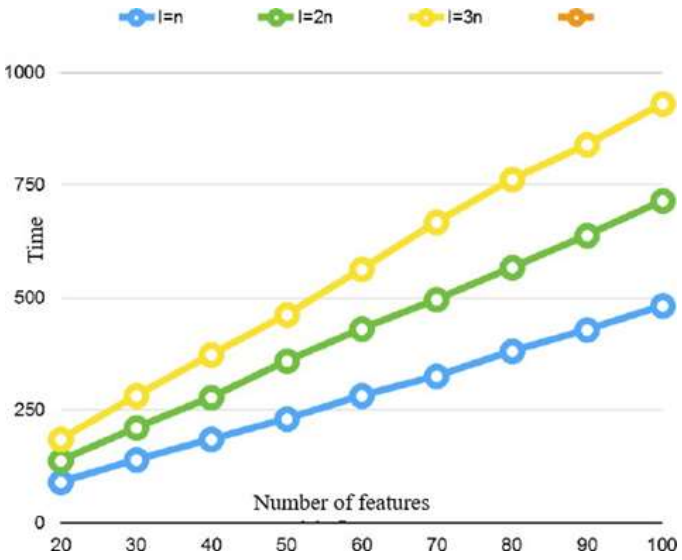

Figure 6: Algorithm execution time diagram - Fairness_Aware for different number of interests (Fast variant of Paillier)

According to Figure 6, it is clear that the execution time of the algorithm increases with increasing security parameter and number of users' interests. In this algorithm, only Decryption is performed. In fact, this algorithm guarantees that none of the users is aware of the comparison result and sends the results directly to the verifier.

Table 4: Algorithm execution time - fairness-Aware for different number of features and security parameter (RSA)

n	I=n	I=2n	I=3n
20	144	209	275
30	212	314	429
40	2943	419	578
50	347	532	726
60	408	630	874
70	506	734	1043
80	580	836	1176
90	665	966	1323

100	764	1057	1464

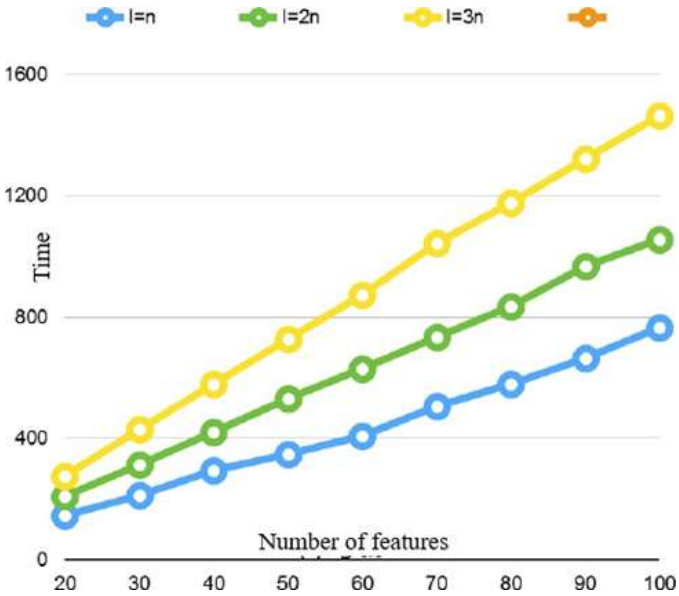

Figure 7: Fairness-Aware algorithm execution time diagram for different number of features (RSA)

According to Figure 7, it is clear that the execution time of the algorithm increases with increasing security parameter and number of user interests. In this algorithm, only the Decryption operation is performed. In fact, this algorithm guarantees that none of the users are aware of the comparison result and sends the results directly to the verifier. As seen before and in the comparisons of the third section, the RSA algorithm is not very successful in the Decryption operation and that is why the execution time of this algorithm has increased compared to before (from 1000 to 1600).

V. CONCLUSION

This research was conducted considering the growth of mobile social networks in the current era and the increasing penetration of these networks into people's personal lives. Personal information in users' profiles is the most important asset of people in cyberspace [26-29]. Considering the penetration of hackers and profit-seeking users into users' personal profiles and the use of users' personal information, it is the most important concern of people in the field of using these networks.

Therefore, in this research, one of the best and most up-to-date security protocols in the field of social networking dating has been introduced, and since this security protocol has been considered in the original article in terms of execution time, an attempt was made to improve the execution time of the algorithm. For this purpose, by introducing the RSA

© 2019 IJSRET

encryption algorithm and replacing it with the Fast variant of Paillier algorithm, it was achieved that the overall execution time of the protocol was reduced by almost half. The importance of this success increased when this improvement was accompanied by another crucial improvement, which was almost 9 times the length of the encryption key in the RSA algorithm, which was 160 bits in the Fast variant of Paillier algorithm, but reached 1024 bits in RSA.

Considering the algorithm and materials presented in this research and the growth of applications such as Wechat, Loopt, and Momo that have the ability to search their surroundings to find new friends, suggestions for further research in this field have been considered.

These suggestions include, study and improve the protocol encryption algorithm, because it is of great importance in the security and speed of the protocol implementation due to its call in the other three algorithms. Revise the Blind Linear Transformation algorithm and integrate this algorithm with the Fairness-Aware algorithm. Remove the verifier to perform comparisons and give results, by changing the overall protocol algorithm to eliminate the possibility of collusion between the verifier and one of the users.

REFERENCES

1. Etuh, E., Bakpo, F. S., and Agozie, H. E. 'Social Media Network Attacks and Their Preventive Mechanisms: A Review', Science Direct, Volume 140,14 (2022).
2. Yue, H., He, S., & Liu, Z. Social Media Users Send Promotional Links to Strangers: Legitimate Promotion or Security Vulnerability? IEEE Access, volume 140 , 14 (2020)
3. Pattnaik, N., Li, S., and Nurse, J. R. C. 'Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter', Science Direct, volume 125 , 15 (2022)
4. Gordhan Jethava a, Udai Pratap Rao b ,Exploring security and trust mechanisms in online social networks: An extensive review, volume 140 ,13 (2023).
5. F. Yang, Y. Wang, F.u. Chunlei, H.u. Chunqiang, A. Alrawais (2020). An Efficient Blockchain-Based Bidirectional Friends Matching Scheme in Social Networks IEEE Access, 8 (2020), pp. 150902-150913, 10.1109/ACCESS.2020.3016986
6. B. N. S. V. R. S. A. Goparaju, Y. S. R. Mutyam, D. V. G. S. Kotha, S. K. Mellacheruvu andS. Kolachana, "Understanding Security and Privacy Issues in Social Media Networks 1," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 1538-1542, doi: 10.1109/ICAAIC60222.2024.10575254.
7. Mohammadi, A. & Hamidi, Hoda. (2018). Analysis and Evaluation of Privacy Protection Behavior and Information Disclosure Concerns in Online Social Networks. International Journal of Engineering, Transactions B: Applications. 31. 1234-1239. 10.5829/ije.2018.31.08b.11.
8. Jain, A.K., Sahoo, S.R. & Kaubiyal, J. Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177 (2021). https://doi.org/10.1007/s40747-021-00409-7
9. K. Puttaswamy et al., Preserving Location Privacy in Geo-Social Applications, IEEE Trans. Mobile Computing,2013
10. ComScore [Online]. Available: http://www.comscoredatamine.com/ Accessed: 4 Apr. 2014
11. Weinstein, E. (2018). The social media see-saw: Positive and negative influences on adolescents' affective well-being. New Media & Society, 20(10), 3597-3623. X.Liang, K.Zhang And X.Shen, SECURITY AND PRIVACY IN MOBILE SOCIAL NETWORKS: CHALLENGES AND SOLUTIONS : IEEE, February 2014
12. M. Motani, V. Srinivasan, and P. Nuggehalli, Peoplenet: Engineering a Wireless Virtual Social Network, Proc. MobiCom, 2005, pp. 243–57
13. Ademiluyi, A., Li, C., & Park, A. (2022). Implications and preventions of cyberbullying and social exclusion in social media: systematic review. JMIR formative research, 6(1), e30286.
14. Kumar Birthriya, S., & Jain, A. K. (2022). A Comprehensive Survey of Phishing Email Detection and Protection Techniques. Information Security Journal: A Global Perspective, 31(4), 411-440.
15. Etuh, E., & Bakpo, F. S. (2022). Social Media Networks Attacks and their Preventive Mechanisms: A Review. arXiv preprint arXiv:2201.03330.
16. Jain, A. K., Sahoo, S. R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177. https://doi.org/10.1007/s40747-021-00409-7
17. Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well- being. Current Opinion in Psychology, 101314.
18. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198, 656-661.
19. I. Mutambik, A. Almuqrin, Y. Liu, M. Alhossayin, and F. H. Qin-tash, ''Gender differentials on

© 2019 IJSRET

information sharing and privacy concerns on social networking sites: Perspectives from users,'' J. Global Inf. Manage., vol. 29, no. 3, pp. 236–255, May 2021

20. L. Floridi, "Soft ethics the governance of the digital and the General Data Protection Regulation", Philosophical Transactions of the Royal Society A, vol. 377, no. 2142, pp. 20180081, 2019.
21. D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms. Reading, MA, USA: Addison-Wesley, 1997.
22. R. Rivest, Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer, unpublished.
23. P. Nyoni and M. Velempini (2013), "An evaluation of online privacy and policies of social networks," 2013 Pan African International Conference on Information Science, Computing and Telecommunications (PACT), Lusaka, Zambia, 2013, pp. 45-49, doi: 10.1109/SCAT.2013.7055087.
24. Liang, Xiaohui & Zhang, Kuan & Shen, Xuemin & Lin, Xiaodong. (2014). Security and privacy in mobile social networks: Challenges and solutions. Wireless Communications, IEEE. 21. 33-41. 10.1109/MWC.2014.6757895.
25. H. Zhu ,S. Du, M. Li And Z. Gao, Fairness-Aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks:IEEE 2013
26. H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, SMART: A secure multilayer credit-Based incentive scheme for delay-tolerant networks, IEEE Trans. Veh. Technol., vol. 58, no. 8,

1. pp. 828_836, Oct. 2009.

27. H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, SLAB: Secure localized authentication and billing scheme for wireless mesh networks, IEEE Trans. Wireless Commun., vol. 17, no. 10, pp. 3858_3868, Oct. 2008.
28. N. Eagle and A. Pentland, Social serendipity: Mobilizing social soft-ware, IEEE Pervas. Comput., vol. 4, no. 2, pp. 28_34, Apr. 2005.
29. Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, ESmallTalker: A Distributed Mobile System for Social Networking in Physical Proximity, in 2010 International Conference on Distributed Computing Systems, Jun. 2010, pp. 468–477

© 2019 IJSRET